G Data InternetSecurity

ユーザーマニュアル

2012/11/01 改定版

本マニュアルの内容と製品セットアップ内のPDFマニュアルの内容は異なる場合があります。

目次

はじめに

この度はG Data 製品をお買い求めいただき、誠にありがとうございます。本マニュアルでは、製品のインストール、コンピュータを不正プログラムから効果的に保護するためのヒントが分かりやすく纏められています。本製品を操作する上でわからないことがでてきたら、まずは、マニュアル、ヘルプファイル、G Data ウェブサイトのFAQなどでご確認ください。

このマニュアルでは、製品のインストール方法と実用的なヒントをまとめています。

※使用している画面は開発中のものを使用しておりますので、実際の画面と異なる場合があります。ご了承ください。

左のアイコン（もしくはF1ボタン）を押すと、オンラインヘルプを呼び出すことができます。

ユーザーサポート

操作方法など、ご購入後の製品に関するお問い合わせは、ユーザーサポートで受付いたします。

※体験版の場合は、ユーザーサポートのご利用はできません。予めご了承ください。

ユーザーサポートの連絡先

問い合わせ先については、登録後のメールをご確認ください。

1. サポート期間
ライセンス有効期間内

2. サポート範囲
製品のご利用の説明、疑問点にお答えするサービスとさせていただきます。以下の場合には、お問い合わせに対してのご回答ができませんので、予めご了承ください。

a) 本製品で保証している動作環境外でのお問い合わせ
b) 本製品ではないもの（ハードウェア・他社製品）に関するお問い合わせ
c) サポート時間外のサポートおよび、指定された方法以外の方法でのサポートのご依頼

3. ユーザーサポートをお受けになる際に

お問い合わせの際は、お客様番号または、レジストレーション番号をご用意いただき、更に質問要点を整理していただいた上で、お問い合わせいただきますようお願いいたします。

インストール

まず本製品をインストールする環境についてご確認ください。本製品を正常に機能させるためには、以下の**動作環境**を満たす必要があります。

動作環境

対応OS	Windows 8 (32bit/64bit) Windows 7 (32bit/64bit) Windows Vista (32bit/64bit) Windows XP [SP2以降](32bit) ※インストールには管理者(Administrator)権限でログインする必要があります。 ※日本語OS環境のみサポート。 ※最新のサービスパックを推奨。
CPU	各OSが推奨するCPU
メモリ	Windows 8/7/Vista：1GB以上 [2GB以上推奨] Windows XP：512MB以上 [1GB以上推奨] ※グラフィックメモリとの共用は除きます。
ハードディスク	1GB以上の空き容量
デバイス装置	CDドライブ（パッケージ版のみインストール時に必要） ※ブートCDの作成・バックアップ時には書き込み可能なCD/DVDドライブが必要です。
ディスプレイ	解像度1024×768ドット、High Color（16ビット、65,536色）以上
その他	InternetExplorer7以上 インターネットに接続可能な環境[ブロードバンド以上を推奨]

※他のウイルス対策ソフトとは併用できません。
※ユーザー登録するためにはPCのメールアドレス（携帯メール不可）が必要です。
新品のコンピュータ、もしくは本製品インストール前に他のウイルス対策ソフトで保護されていたコンピュータでは、次のステップを参考に本製品をインストールしてください。それ以外の場合やコンピュータがウイルスに感染している疑いがある場合は、インストール前にブートスキャンを実行することをお勧めします。 ブートスキャンの方法については、ブートスキャンの流れを参照してください。

ステップ 1

本製品はCD/DVDメディア以外に、ダウンロード形式でも販売されています。それぞれのインストール方法は次のとおりです。

- **CD/DVD製品の場合**: 本製品CD/DVDをCD/DVDドライブにセットします。暫くすると、自動的にインストール開始画面が開きます。
- **ダウンロード販売製品の場合**: ダウンロードしたファイルをダブルクリックします。暫くすると、インストール開始画面が開きます。

注意！
他のウイルス対策ソフトがコンピュータにインストールされている場合もしくは、されていた場合は、ソフトのアンインストールを行った後に、各社の提供する完全削除ツールで関連データの削除を行ってください。
ウイルス対策ソフトはシステム深くに配置されるため、通常のアンインストールではすべてのデータが消えない事がほとんどで、これが動作不良の原因になる場合があるためです。

ステップ 2

インストール画面の**「インストール」**をクリックしてインストールを開始します。

ステップ 3

製品版としてインストールするか、体験版としてインストールするかを選択します。

- **製品版**: 製品版を購入した場合は、ここを選択します。
- **体験版として試用**: 本製品の無料体験版を利用する場合は、ここを選択します。なお、体験版を利用するには、氏名とメールアドレスの入力が必要です。入力されたメールアドレスには、アクセスデータが送付されるので、必ず有効なメールアドレスを入力してください。

ステップ 4

インストール中に**ユーザー認証**を行い、プログラムの機能をすべて使用できるようにします。

- **レジストレーション番号を登録**: 製品を新規購入された方は、ここを選択し、購入製品のレジストレーション番号を入力してください。パッケージ版を購入された場合は、レジストレーション番号は同梱の用紙に記載されています。ダウンロード版を購入された場合は、レジストレーション番号はメールで送信されています。

  レジストレーション番号を入力して、製品が正常に認証されると、更新ファイルをロードできるようになります。複数台版やライセンスの移行で必要になるアクセスデータは、認証後に G Data から送付されるメールに記載されています。アクセスデータは厳重に保管してください。

  入力したレジストレーション番号で認証できない場合は、まず入力ミスの可能性がないか確認してください。更に問題が解決できない場合は、ユーザーサポートにお問い合わせください。

- **アクセスデータを入力**: アクセスデータ（ユーザー名とパスワード）を使って、認証します。本製品を再インストールしたり、ライセンス権限を他のコンピュータから移行した場合は、ここを選択してアクセスデータを入力してください。

  アクセスデータは初回認証（レジストレーション番号を入力）後に G Data から送付されたメールに記載されています。製品には同梱されていません。

  アクセスデータを紛失したり忘れた場合は、**アクセスデータを紛失した場合**をクリックしてください。ブラウザが自動的に起動して G Data のサポートページが開きます。サポートページに記載されている手順に沿って手続きをし、アクセスデータを再確認してください。※アクセスデータの再確認では、レジストレーション番号が必要です。またアクティベーション時に登録から、メールアドレスを変更した場合は、ユーザーサポートへお問い合わせください。

  ※複数台版を購入した場合で、1台目のコンピュータを登録し、2台目以降のコンピュータにインストールする場合は、この項目を選択し1台目の登録で発行されたアクセスデータを入力してください。

- **後で認証を行う**: 後で製品を認証する場合は、ここを選択します。インストール後はできるだけ早く認証の手続きをしてください。インストール後の認証方法は、更新の実行するか、**設定**アイコンをクリックして、**アンチウイルス**の**更新**領域から可能です。

  ウイルス対策ソフトは、定期的な更新を行うことでコンピュータの保護を実現します。認証しない状態でプログラムを利用し続けると、コンピュータを適切に保護できません。

ステップ 5

インストール後にコンピュータを再起動する必要がある場合があります。その場合は、再起動後に本製品の機能が利用できるようになります。

インストールの起動画面が自動的に表示されない場合
Windowsの自動再生機能が無効になっているため、CD/DVD、USBメモリから本製品のインストール画面が自動的に起動できない可能性があります。

- 自動再生の画面が表示される場合は、**AUTOSTRT.EXE の実行**をクリックしてください。

- 自動再生の画面が開かない場合は、Windows Explorerから本製品を探して、Setup もしくは Setup.exe をダブルクリックしてください。

これで、本製品のインストール画面が表示されインストールを開始できるようになります。

インストール後

G Data ショートカット: 左のアイコンがデスクトップ上に作成されます。本製品のインターフェースを開くには、このアイコンをダブルクリックします。セキュリティセンターの利用方法については、セキュリティセンターに詳しく記載しています。

G Data アイコン: ユーザーの操作が必要になると、タスクバーのG Data アイコンからお知らせします。その他の情報は、G Data アイコンの項を参照してください。

クイックスキャン: ファイルやフォルダで簡単なウイルスチェックをする場合は、プログラム画面を起動する必要はありません。対象の上で右クリックし、**ウイルススキャン**を選択すると、スキャンが実行されます。

G Data シュレッダー: インストールでシュレッダーを選択すると、デスクトップ上にシュレッダーアイコンが作成されます。シュレッダーを使ってファイルを完全に削除するには、ファイルをシュレッダーのアイコン上に移動するか、ファイルの上で右クリックして、シュレッダーを選択します。一旦シュレッダーでファイルを削除すると、ファイルは復元不可能になります。※シュレッダー機能は、G Data **アンチウイルス**には含まれていません。

本製品をインストールしてコンピュータを再起動した際に、Windows が起動しない場合: まずCD/DVDドライブに本製品CDが挿入されたままではないか確認してください。本製品CDは、ブートスキャン機能を搭載しているので、コンピュータの設定によっては、Windows 起動前にブートCD が起動している可能性があります。製品CDがCD/DVDドライブに挿入されていた場合は、CDを取り出し、コンピュータを再起動してください。Windows が通常通りに起動します。

ブートスキャンに関する詳細は、**ブートスキャンの流れ**の項を参照してください。

セキュリティセンター

本製品を起動すると立ち上がるセキュリティセンター画面では、各機能のステータスを確認したり、操作を実行できます。

※画面はトータルプロテクションのものです。

セキュリティステータスのアイコンを使うと、ボタン操作ひとつだけで、コンピュータの保護状況を簡単に改善できます。

「対策」ボタンでは、ボタン操作１つだけで、コンピュータを守るための対策が提案されます。コンピュータの保護が完全に改善されると、対策ボタンは無効になります。セキュリティステータスが再び緑色に戻るまで、対策を順に選択し、保護レベルを改善してください。セキュリティステータスが緑色になると、コンピュータの保護が最新の状態になっていることを意味しています。

ステータス情報には、次のようなマークがあります。

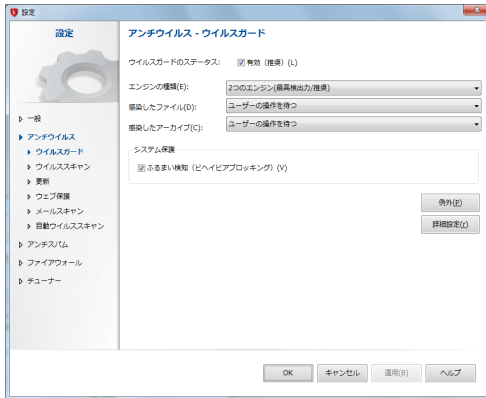
緑色のチェックマーク＝すべて良好（システムは保護されています）

赤色のマーク＝今すぐに改善が必要（システムが危険にさらされている可能性があります）

黄色のマーク＝近いうちに改善が必要

灰色のマーク＝このセキュリティ機能は無効

セキュリティセンター画面の右上に配置されているボタンからは、次のような操作ができます。

設定: 各プログラムの様々な設定を確認したり、変更したりできます。

詳細は設定の項を参照してください。

設定の隣にある**その他**をクリックすると、次の機能が利用できます。

ヘルプ: プログラムに関するヘルプファイルを呼び出します。ヘルプファイルはF1ボタンから呼び出すことも可能です。

ログ: ワクチン更新やウイルススキャンなど実行した操作に関するログを表示します。

ブートCD を作成: ブートCDは、感染済みのコンピュータからウイルスを駆除するには大変効果的です。特に本製品をインストールする前に、ウイルス対策ソフトをインストールしていなかったコンピュータには、ブートスキャンをお勧めします。ブートCD の作成方法や使用方法は、ブートスキャンの流れを参照してください。

ブートCDの作成機能が見つからない場合: この機能がインストールされていない可能性があります。製品CDもしくはセットアップを起動し、ダイアログに従って、**ブートCDを作成**を追加してください。

プログラムの更新: プログラム更新が利用できる場合は、ここからプログラムファイルを更新できます。

インターネット更新ができない場合は、**更新**の項を参照してください。

情報: プログラムのバージョン情報を表示します。バージョン番号は、ユーザーサポートへの問い合わせ時に必要になることがあります。

ライセンス

ワクチン更新が利用できるライセンスの有効期限を確認できます。

ウイルス対策ソフトにおいて、更新は非常に重要です。インターネット更新は必ず定期的に実行し、製品を常に最新の状態に保つように心がけてください。本製品はお手元のライセンスの有効期間が切れる前に、自動的にライセンス延長についてお知らせします。ライセンスの延長は、以下の手順で簡単に手続きできます。

ライセンスの有効期間が切れた場合

ライセンス期限が切れる数日前から、タスクバーにその旨を知らせるバルーンが表示されます。 このバルーンをクリックすると、ダイアログが開くので、ダイアログの説明に従い、簡単に更新をインターネット経由でできます。

CPU使用率

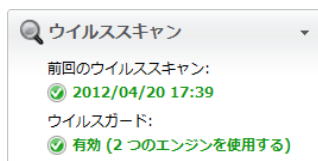
CPU使用率モニタでは、本製品の動作中にコンピュータに掛かっている負荷を表示します。上段が本製品のCPU使用率、下段はシステム全体のCPU利用率です。通常、ウイルススキャン中には負荷が高くなりますが、普段の負荷はほとんどありません。

初期設定では、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみスキャンを行う、**アイドリングスキャン**機能が有効になっています。スクリーンセーバーのように動作しますので、ウイルススキャンの負荷により作業を妨げる事を防ぐ事ができます。

もし特定のアプリケーション（例: ビデオ編集プログラム）で CPU使用率が上がる場合には、そのアプリケーションをウイルスガードで例外設定すると改善する可能性があります。ウイルスガードの例外設定については、**ウイルスガード**の項を参照してください。

- ウイルススキャン: 定期的あるいは特定タイミングで、ハードディスクディスク等に含まれるシステム内にウイルスが潜んでいないかどうかをチェックします。
- ウイルスガード: ウイルスを常時監視するリアルタイムスキャン機能

ウイルススキャン

最後にウイルススキャンを実行した日時やウイルスガードの有効/無効など、ウイルススキャンに関する情報が表示されます。

前回のスキャン/アイドリングススキャン

前回コンピュータでウイルススキャンされた日時を表示します。ステータス情報が赤色で表示されている場合は、できるだけ早くウイルススキャンを実行してください。ウイルススキャンを今すぐに実行するには、ウイルススキャンの文字をクリックするとプルダウン表示される**「コンピュータをスキャン」**をクリックします。スキャンが完了すると表示色が緑色に変わります。

ウイルススキャンの詳細やウイルス感染が検出された場合の対処方法については、**ウイルススキャンの流れ**の項を参照してください。

アイドリングスキャンは、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみ自動的に起動するスキャン機能です。アイドリングスキャン中にユーザーがコンピュータを利用すると、実行中のスキャンはすぐに休止状態となります。
アイドリングスキャンを次回の実行予定よりも先にを実行したい場合は、**アイドリングスキャンを実行**を選択してください。逆にアイドリングスキャン自体を使用したくない場合は、**アイドリングスキャンを無効にする**を選択してください。

アイドリングスキャンは初期設定では有効になっています。

アイドリングスキャンを無効にした場合は、**自動ウイルススキャン**を利用して定期的なスキャンを行う事をお勧めします。

ウイルスガード

ウイルスガードは常時有効にしておいてください。ウイルスガードを一旦無効にする場合は、ステータス情報をクリックするとプルダウン表示される**ウイルスガードを無効にする**をクリックするか、タスクバー上の G Data アイコン上で右クリックし、**ウイルスガードを無効にする**を選択します。

本製品には、**ウイルススキャン**と**ウイルスガード**という2種類の性質の異なった保護方法が搭載されています。

ウイルスガードとは
ウイルスを常時監視するリアルタイムスキャン機能で、書き込みおよび読み取り処理を監視します。あるプログラムが不正な機能を実行したり、不正ファイルを拡散しようとすると、ウイルスガードがこれを防ぎます。ウイルスガードは最も重要なウイルス対策の１つです。常に有効にしておいてください。

ウイルススキャンとは
補助的なウイルス保護機能で、オンデマンドスキャンとも呼ばれます。この機能はシステム内にウイルスが潜んでいないかどうかをチェックします。ウイルススキャンは、本製品をインストールする前や、ウイルスガードを無効にしていた間にシステムに感染していたウイルスなどを検出できます。コンピュータを利用しない時などに、定期的かつ自動的にウイルススキャンを実行することをお勧めします。

プルダウンメニュー

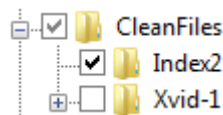
ウイルススキャンの上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

コンピュータをスキャン: ウイルス感染の疑いがある場合など、スケジュールスキャンとは関係なく、今すぐにコンピュータをスキャンする必要がある時は、ここをクリックします。クリック後は、ただちにスキャンが開始されます。**ウイルススキャンの流れ**の項も参照してください。

メモリおよびスタートアップをスキャン: 実行中のすべてのプロセスに対して、プログラムファイル および DLL（プログラムライブラリ）をスキャンします。不正プログラムが見つかった場合は、**メモリとスタートアップ領域**から不正プログラムをすぐに除去します。このスキャンは比較的短時間で完了できるため、自動ウイルススキャンなどと一緒に定期的に実行することをお勧めします。

※この機能は、保存データの定期的なウイルススキャンに代わるものではなく、それを補完するものです。

フォルダ/ファイルをスキャン: 選択したドライブ、フォルダ、またはファイルがウイルスに感染していないか調べます。この操作をクリックすると、フォルダとファイルの一覧が表示されます。個々のファイルにターゲットを絞ってスキャンしたり、フォルダ全体のウイルススキャンを行うことができます。

フォルダツリーでは、「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。ウイルススキャンは、チェックボックスにチェックが入っているフォルダまたはファイルに対して、行われます。一部スキャンされないファイルがあるフォルダには、グレーのチェックマークが表示されます。

リムーバブルメディアをスキャン: CD/DVD-ROM、フロッピーディスク、メモリカード、USB メモリなどをスキャンします。この機能を選択すると、コンピュータに接続されているすべてのリムーバブルメディア（トレイに挿入済みのCD/DVD-ROM、メモリカード、または USB経由で接続中の外付けハードディスクやUSB メモリ）をスキャンします。ただし、本製品は書き込み不可のメディアに対してウイルス除去できません。スキャン結果にウイルス検出のログが作成されるだけですので、ご注意ください。

ルートキットをスキャン: ルートキットとは、従来のウイルス検出方法では検出が困難な不正プログラムです。この機能を使うと、ハードディスク内の全データすべてをスキャンすることなく、ターゲットをルートキットに絞ってスキャンします。

アイドリングスキャンを無効にする: アイドリングスキャンは、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみ自動的に起動するスキャン機能です。アイドリングスキャン中にユーザーがコンピュータを利用すると、実行中のスキャンはすぐに休止状態となります。

アイドリングスキャンを無効に設定しても、コンピュータはウイルスガードによって常時保護されます。アイドリングスキャンは、オンデマンドのウイルススキャンを手動で開始した場合などに便利です。

ウイルスガードを無効にする: 必要に応じてウイルスガードを無効にしたり有効にしたりできます。大量のデータをハードディスク上のある場所から別の場所にコピーしたり、多くのメモリを必要とする演算プロセス（DVD のコピーなど）を実行する時には、ウイルスガードを無効にすることをお勧めします。

※ウイルスガードは、必要な時にだけ無効にしてください。また、ウイルスガードが無効に設定されている間は、できるだけインターネットには接続しないようにし、CD、DVD、メモリカードまたは USB メモリなどに保存されている、スキャンをしたことのないデータにはアクセスしないように注意してください。

隔離: 隔離領域では、感染ファイルは暗号化されて保存されます。これにより、検出されたウイルスによる被害は拡大を防止できます。詳細については、隔離でできることの項を参照してください。

設定: ウイルス保護の設定領域に移動します。詳細については、設定 - アンチウイルスの項を参照してください。

更新

ワクチン更新に関する情報が表示されます。

前回のワクチン更新

ここでは、最後にインターネットからワクチンをダウンロードした日時が表示されます。ステータス情報が赤色で表示される場合には、できるだけ近いうちに、ワクチン更新を実行してください。ワクチンを更新するには、表示されているステータス情報の上でクリックし、プルダウン表示される**ワクチンの更新**を選択します。

自動更新

ここには、次回のワクチン更新までの時間が表示されます。

> ワクチンとは
> ウイルスの特徴を検出するためデータが収められた、ウイルス対策ソフトのおいて非常に重要な要素のひとつです。ワクチンは常時更新されています。使用するワクチンのバージョンが古くなると、コンピュータの保護レベルが大幅に低下します。ワクチンは必ず定期的に更新しましょう。

プルダウンメニュー

更新の上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

ワクチンの更新: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。

自動更新を無効にする: 自動更新を無効にする場合は、ここをクリックします。特種なケースを除いては、自動更新は常に有効にしておいてください。

設定: 更新の設定領域に移動します。詳細については、設定 - アンチウイルスの項を参照してください。

ウェブ保護

インターネット利用中の保護を提供する**ウェブ保護**の有効／無効を切り替えます。ウェブ経由での感染が増加している現在、ウェブ保護は感染防止のための重要な機能です。ウェブ機能を有効にすると、ウェブサイト経由の感染やフィッシング詐欺などの脅威から保護できます。

インターネット閲覧中にウェブサイトが本製品によって脅威として検出されると、サイトの閲覧はブロックされ、ブラウザ画面に警告が表示されます。

Windows 8 の Modern UI 用ブラウザ上でウェブ保護が動作した場合は、デスクトップを表示して検出されたウイルスへの対応を決定する必要があります。

プルダウンメニュー

ウェブ保護の上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

例外を設定: ウェブ保護は、不正コードが仕掛けられたウェブサイト、またはフィッシングなどの詐欺サイトからコンピュータを保護する機能です。

なお、ウェブ保護を有効にすると、安全なサイトであるにも関わらず、ウェブページが正しく表示されないことがあります。そのような場合は、このページのアドレスをホワイトリストに例外登録してください。これにより、ウェブ保護がブロックしていたページが閲覧できるようになります。詳細については、例外の項を参照してください。

ホワイトリスト: ユーザーが脅威ではないと判断したサイトで、ここに登録されたサイトに対するチェックは行われません。

ウェブ保護を無効にする: ウェブ保護を無効にすると、ウェブサイトのチェックが無効になるため、ウェブサイトから大量にデータをダウンロードする際などにダウンロード時間を省略できます。また、ウェブ保護が無効中の状態も、ウイルスガードがコンピュータを感染から守ります。しかし、例外的ケースを除いては、ウェブ保護は有効に設定することをお勧めします。

設定: ウェブ保護の設定領域に移動します。詳細については、設定 - ウェブ保護 の項を参照してください。

メール保護

メール送受信時のウイルスからコンピュータを保護する**メール保護**の有効／無効を切り替えます。メール保護機能は、送受信されるメールの内容や添付ファイルをスキャンし、ウイルス感染を防ぎます。ウイルスが検出された場合は添付ファイルを削除、もしくはウイルスの駆除を行います。

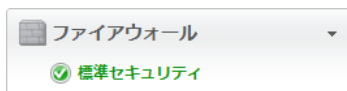
Microsoft Outlook には、専用プラグインがインストールされます。このプラグインは、メールスキャンで設定できる POP3/IMAP ベースの保護を提供し、これにより、Outlook 上でのウイルスチェックがより簡単にできるようになります。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの [ツール] > [フォルダのウイルスをスキャン] を選択します。

プルダウンメニュー
メール保護の上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

メール保護を無効にする: メールのスキャンを行いたくない場合は、ここを選択してください。ただし、その場合はメール経由のセキュリティリスクが大きく増えますので、特別な場合を除いてメール保護は有効に設定しておくことをお勧めします。

設定: メール保護の設定領域に移動します。詳細については、設定 - メールスキャン の項を参照してください。

ファイアウォール

ファイアウォールは、外部の不正侵入からコンピュータを防御するための保護機能です。ファイアウォールは、インターネットまたはネットワークとコンピュータ間の送受信データを監視します。権限なしでの、コンピュータへのデータ書き込みやダウンロードを検知すると、ファイアウォールが警告を発し、権限のないデータ交換を阻止します。

プルダウンメニュー

ファイアウォールの上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

ファイアウォールの設定: ファイアウォール領域のウィンドウが開き、ファイアウォールのステータス確認、詳細設定、ログ表示などができます。

オートパイロットを無効にする: オートパイロットは、ファイアウォールが許可／ブロックするアプリケーションを自動的に判断し制御する機能です。通常は、この機能は有効にして利用することをお勧めします。

オートパイロットを無効にした状態でファイアウォールを使用する場合は、プログラムにルールを学習させ、ネットワーク環境に合わせて設定していく必要があります。上級者ユーザー以外は、オートパイロットを無効にしないでください。

ファイアウォールを無効にする: 必要に応じて、ファイアウォールを無効にします。

※コンピュータがインターネットやネットワークと接続されている環境では、不正な攻撃や侵入から保護されなくなります。ご注意ください。

設定: ファイアウォールの設定領域に移動します。詳細については、**設定 - ファイアウォール**の項を参照してください。

アンチスパム

スパム保護は、迷惑な広告メールや大量のスパムメールに対する対策機能です。G Data のスパム保護は、緻密に設定された判断基準をもとにスパム判定を行うので、迷惑メールや迷惑メール送信者を効果的にブロックします。

プルダウンメニュー

スパム保護の上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

ログ: スパム: スパムと判断されたメールに関する情報が一覧で表示されます。 **「更新」**をクリックすると、ステータス情報を更新できます。対象を選択して**「削除」**を押すと、指定したメールのログを削除できます。なお、ここで削除しても、メールプログラムで受信した実際のメールは削除されません。

「ホワイトリストに登録」では、選択したメールの送信者をホワイトリストに入れ、それ以降はこの送信者からのメールに対するスパムチェックは省略されるようになります。逆に**「ブラックリストに登録」**へ移動されると、この送信者に対するメールは、以降、より入念なスパムチェックが行われるようになります。

ログ: スパム以外: スパムではないと判断されたメールに関する情報が一覧で表示されます。 **「更新」**をクリックすると、ステータスを更新できます。対象を選択して **「削除」**を押すと、指定したメールのログを削除できます。なお、ここで削除しても、メールプログラムで受信した実際のメールは削除されません。

ホワイトリスト: 特定の送信者からのメールアドレスやドメインをスパム扱いしないように設定できます。「ホワイトリスト」に登録するには、**アドレス/ドメイン**の欄にスパム扱いしたくない**メールアドレス**（例：newsletter@gdata.co.jp）または**ドメイン**（例：gdata.co.jp）を入力して、**「追加」**をクリックします。そうすると、入力された送信者またはドメインからのメールは、スパムではないと判定されるようになります。

また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをホワイトリストに追加できます。インポートするリストには、アドレスおよびドメインが 1 件 1 行ずつ、上から順に入力されている必要があります。データフォーマットは、Windows の「メモ帳」で作成できるようなテキスト形式（txt ファイル）を使用します。

「エクスポート」からは、上述のホワイトリストをテキスト形式で書き出します。

ブラックリスト: 特定の送信者からのメールアドレスやドメインをスパム扱いに設定できます。ブラックリストに登録するには、**アドレス/ドメイン**の欄にスパム扱いとする**メールアドレス**（例：newsletter@spam.co.jp）または**ドメイン**（例：spam.co.jp）を入力して、**「追加」**をクリックします。そうすると、入力された送信者またはドメインからのメールは、自動的にスパムと判定されるようになります。

また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをブラックリストに追加できます。インポートするリストには、アドレスおよびドメインが 1 件 1 行ずつ、上から順に入力されている必要があります。データフォーマットは Windows の「メモ帳」で作成できるような、テキスト形式 (txt ファイル) を使用します。

「エクスポート」からは、上述のブラックリストをテキスト形式で書き出します。

スパム保護を無効にする: スパム保護を無効します。コンピュータでメールを利用しない場合などに、この機能を利用してください。

設定: スパム保護の設定領域に移動します。詳細については、設定 - アンチスパム の項を参照してください。

フィルタリング

フィルタリングは、ウェブサイトを一定の基準で評価判別して選択的に排除したり、コンピュータの利用時間に制限をかける機能です。

フィルタリング機能は、標準インストールではインストールされません。フィルタリング機能を追加したい場合は、製品CD/DVDやセットアップを展開して、追加インストールできます。

プルダウンメニュー

フィルタリングの上でクリックすると、操作一覧がプルダウン表示され、ここから操作を直接実行できます。

フィルタリングの設定: フィルタリング領域のウィンドウが開き、フィルタリングのステータス確認、詳細設定、パーソナルフィルタやログの表示などができます。

有効にする: アドミニストレーターもしくは他のユーザー用のフィルタリングを有効／無効にします。セキュリティ設定の編集は、フィルタリング領域のウィンドウ上で設定します。

フィルタリング機能を利用するには、ウェブ保護の**インターネットコンテンツ（HTTP）のスキャン**にチェックが入っている必要があります。これを確認するには、セキュリティセンター画面の右上にある**設定**を選択し、表示される機能群から**ウェブ保護**を選択し、**インターネットコンテンツ（HTTP）**の領域で確認してください。

設定

プログラム画面を起動すると、画面右上に**設定**ボタンが配置されています。ここをクリックすると、本製品に搭載されている機能の設定項目を確認したり、変更したりできます。

一般

ここでは、簡易設定などを行えます。

セキュリティ / パフォーマンス

この画面では、コンピュータの性能に応じて簡易的にセキュリティ設定を最適化できます。下のメーターでは、それぞれの設定が及ぼすパフォーマンスやセキュリティ性能への影響を確認できます。まず簡単に動作の調整を行いたい、という場合にはこの機能を使用すると便利です。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

アンチウイルス

ウイルス対策機能に関する様々な設定を確認したり、変更したりできます。

ウイルスガード
ウイルスガードの**設定**では、以下の設定が可能です。

- **ウイルスガードのステータス**: ウイルスガードの有効／無効を設定します。
- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。
- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、感染ファイルの処理方法についてユーザーに確認が行われます。なお、データを最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。
- **感染したアーカイブ**: **アーカイブファイル**（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイブは、**ユーザーの操作を待つ**を選択し、検出の度に処理方法をユーザーに選択させることをお勧めします。
- **システム保護**
ふるまい検知（ビヘイビアブロッキング）：コンピュータ上のWindows のレジストリやHOSTSファイルへのアクセスやネットワークアクティビティを監視します。ふるまい検知は、Windows のレジストリやHOSTSファイル へのアクセスやネットワークアクティビティを監視することにより、通常のウイルススキャンで検出できなかった典型的な不正プログラムの振舞いをするプロセスを検出します。

例外
ウイルスガードによるスキャンが不要なドライブ、ファイル、フォルダをスキャンの対象から除外する設定が可能です。例外を設定するには、以下の手順に沿って行います。

1. **「例外」**をクリックします。
2. **ウイルスガード用の例外設定**のダイアログ画面が開くので、**「新規作成」**をクリックします。

3 次の**例外設定**の画面で、次に除外する対象をドライブ、フォルダ、ファイルから選択します。

4 ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力、もしくは、「 ... 」をクリックして対象を指定します。

ファイルを指定するには、完全なファイル名を入力します。ファイルを入力する際はワイルドカードを使用できます。

ワイルドカードの機能は次のとおりです。

- **疑問符 (?)**：任意の1文字に代わるワイルドカード
- **アスタリスク (*)**：文字列全体に代わるワイルドカード

例：　拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力します。連続性のある名前のファイル（text1.doc、text2.doc、text3.doc など）などを保護するには、「**text?.doc**」と入力します。

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルスガードのスキャンをカスタマイズできます。また、作成した例外設定は、**ウイルスガード用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ「**編集**」 と 「**削除**」から可能です。

詳細設定

「**詳細設定**」からは、ウイルスガードが行うスキャンの詳細内容を確認したり、変更できます。

- **モード**: ファイルをスキャンするタイミングを、**読み込み/書き込み時にスキャン**、 **読み込み時にスキャン**、もしくは**実行時にスキャン**から選択します。
- **ネットワークアクセスのスキャン**: ネットワークアクセスで不正プログラムをスキャンします。自身のコンピュータを、ネットワーク経由でウイルス対策がされていない第三者のコンピュータと接続する場合には、この機能を有効にしてください。コンピュータがネットワークに未接続で使用している環境では、この設定は有効にする必要はありません。ネットワーク上のすべてのコンピュータにウイルス対策ソフトがインストールされている場合にも、この設定は無効にしてください。有効にすると、重複スキャンが行われることがあり、動作速度の低下につながります。

- ヒューリスティック: ワクチンに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断することもあります。
- アーカイブのスキャン: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- メールアーカイブのスキャン: メールアーカイブをスキャンします。なお、本製品は、メールの送受信する際にスキャンを実行しているので、通常はこの機能は無効にしていても問題はありません。メールアーカイブのスキャンは、アーカイブのサイズによっては数分間かかることがあります。
- システム起動時にシステム領域をスキャン: システム領域のスキャン実行タイミングをシステム起動時に設定します。この設定、もしくはメディアの変更時にシステム領域をスキャンのいずれかは常に有効にし、スキャン対象から除外しないでください。
- メディアの変更時にシステム領域をスキャン: システム領域のスキャン実行タイミングをメディアの変更時（新しい CD-ROM など）に設定します。この設定もしくはシステム起動時にシステム領域をスキャンのいずれかは常に有効にし、スキャン対象から除外しないでください。
- ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、勝手に高額なインターネット接続を確立したり、閲覧履歴やキーボードへの入力（パスワードなど）を盗みだしたりします。
- 新しいファイルと編集したファイルのみスキャン: この機能を有効にすると、以前スキャンしたことがあり、その際に安全と判断されたファイルのスキャンを省略します。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を向上させることができます。

ウイルススキャン
ウイルススキャンに関する基礎的なプログラム設定を行います。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。
- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、ウイルスが検出されるとウイルスと感染ファイルについてのログが残されます。最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。
- **感染したアーカイブ**: **アーカイブファイル**（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイブでは、 **ログを残すのみ**を選択し、検出の度に処理方法をあとから選択することをお勧めします。
- **高システム負荷時にはウイルススキャンを停止**: ユーザーがコンピュータを使用していない状態にだけ、スキャンを実行します。スキャン実行中にユーザーがコンピュータを再び使用すると、スキャンは中断されます。中断されたスキャンは、ユーザーがコンピュータを使用しない状態になった場合に再開されます。

例外
ウイルススキャンによるスキャンが不要なドライブ、ファイル、フォルダをスキャンの対象から除外する設定が可能です。例外を設定するには、以下の手順に沿って行います。

1. **「例外」**をクリックします。
2. **ウイルススキャン用の例外設定**のダイアログ画面が開くので、**「新規作成」**をクリックします。
3. 次の**例外設定**の画面で、除外する対象をドライブ、フォルダ、ファイルから選択します。

4 ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力、もしくは、**「 ... 」**をクリックして対象を指定します。

ファイルを指定するには、完全なファイル名を入力します。ファイルを入力する際はワイルドカードを使用できます。

ワイルドカードの機能は次のとおりです。

- **疑問符 (?)** : 任意の1文字に代わるワイルドカード
- **アスタリスク (*)** : 文字列全体に代わるワイルドカード

例：　拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力します。連続性のある名前のファイル（text1.doc、text2.doc、text3.doc など）などを保護するには、「**text?.doc**」と入力します。

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルススキャンをカスタマイズできます。また、作成した例外設定は、**ウイルススキャン用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ**「編集」** と **「削除」**から可能です。

アイドリングスキャンでも例外を有効にする: アイドリングスキャンは、ユーザーがコンピュータを利用しない時に自動的に起動するスキャン機能です。アイドリングスキャン中に、ユーザーが再び作業をはじめると、実行中のスキャンは中断されます。ユーザーはスキャンによるコンピュータ速度の低下に悩まされることはありません。ここではアイドリングスキャンでスキャン対象から除外するファイルやフォルダを指定します。

詳細設定

「詳細設定」からは、**ウイルススキャン**によるスキャンの詳細内容を確認したり、変更したりできます。

- **ファイルの種類**: ウイルススキャンの対象になるファイルタイプを指定します。**プログラムファイルとドキュメントのみ**を選択すると、速度優先でウイルススキャンします。

- **ヒューリスティック**: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断してしまうケースもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。
- **システム領域のスキャン**: システム領域をスキャンします。この設定は常に有効にしておいてください。
- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、勝手に高額なインターネット接続を確立したり、閲覧履歴やキーボードへの入力（パスワードなど）を盗みだす恐れがあります。
- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。
- **新しいファイルと編集したファイルのみスキャン**: この機能を有効にすると、以前スキャンしたことがあり、その際に安全と判断されたファイルのスキャンを省略します。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を向上させることができます。
- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右上の**その他機能**をクリックし、プルダウンで表示されるメニューから**ログ**を選択します。

更新
ワクチンやプログラム更新が機能しない場合には、この領域で設定を確認してください。更新を利用するには、有効な**アクセスデータ（ユーザー名とパスワード）**が入力されている必要があります。

アクセスデータは、本製品を認証した時に、登録先メールアドレスに送信されています。

本製品をインストールされた後、まだユーザー認証をされていない場合には、**「ユーザー認証（初回用）」**をクリックして認証手続きを行ってください。レジストレーション番号は表示された入力欄に入力します。

バージョン確認
この設定には、通常チェックを入れたままにしておきます。エンジンが破損したり、誤ってワクチンファイルを削除した場合などにのみ、この設定を無効にして更新をしてください。

自動的にワクチン更新を実行（推奨）
デフォルト設定の自動更新を利用しない場合にチェックを外します。長い期間ワクチンが更新されない場合、コンピュータの保護率が大きく損なわれますので、この設定の解除は特別な場合のみ行ってください。もし更新間隔が短すぎる場合は、必要に応じて実行頻度を調節してください。
実行頻度内の、毎日（インターネット接続時）、もしくは毎時（インターネット接続時）という設定は、コンピュータがインターネット接続中かどうかを判断し、インターネットに接続している場合のみ更新処理を行う設定です。これはコンピュータを外へ持ち出している場合などに適した設定で、不必要な処理を減らす事ができます。

ログを作成
ワクチン更新やウイルス検出などのログを記録します。ログを閲覧するには、起動画面の右上にある**その他の機能**をクリックし、プルダウンで表示されるメニューから**ログ**を選択してください。

ユーザー認証
この画面に発行されたアクセスデータを入力する事で、ワクチン更新等が利用できるようになります。複数台版を購入した場合で、2台目以降のコンピューターを使用する際は、1台目の登録で発行されたアクセスデータをここに入力することでワクチン更新等が利用できるようになります。

まだ本製品を登録していない場合は、ここから**レジストレーション番号**と**ユーザーデータ**を入力して認証を行うことができます。ボックス製品を購入された場合は、レジストレーション番号はユーザー登録用紙に記載されています。ダウンロード版を購入された場合は、メールで送信されています。

製品を認証するには、**「ユーザー認証（初回用）」**をクリックすると現れる画面に、**レジストレーション番号、姓名、メールアドレス（PC用）**を入力し、**「登録」**をクリックします。認証が正常に行われると、**「登録に成功しました。アクセスデータは自動的に本製品に登録され、メールでもアクセスデータが送信されます。」**というメッセージが表示されます。**「OK」**をクリックして、この画面を閉じます。

認証後は、ユーザー名とパスワードの入力欄に生成されたアクセスデータが自動的に入力されます。これで更新を実行できるようになります。

※登録されたメールアドレスにアクセスデータが送信されます。メールアドレス入力の際は、誤入力のないようにご注意ください。アクセスデータは、複数台版を購入され、2台目以降のPCを認証する場合や再インストールの際に必要です。

認証用の更新サーバーにログオンできない場合
ブラウザなどでインターネットに正常に接続されているか確認してください。ブラウザでインターネット閲覧できるにもかかわらず更新がロードできない場合は、プロキシサーバーに問題がある可能性があります。この場合は、**インターネット設定**をクリックしてください。

インターネット設定
プロキシサーバー を使用する環境では、**プロキシサーバーを使用**にチェックを入れてください。この設定は、インターネット更新が正常に機能しない場合にのみ変更します。プロキシサーバーの入力欄で入力する情報については、システム管理者またはインターネット接続プロバイダに確認してください。

プロキシサーバー
プロキシサーバーは、ネットワーク内に存在するPCの代理でインターネットへ接続するコンピュータです。インターネット更新が機能しない場合は、まずブラウザなどでインターネットに正常に接続されているか確認してください。

地域では、更新データのダウンロード先サーバーを選択します。ユーザーがコンピュータを使用している国／地域を選択します。日本国内で利用する場合は、デフォルト設定の**アジア（日本）**のままでご利用ください。

ウェブ保護
ウェブ保護では次の設定が可能です。

- **インターネットコンテンツ（HTTP）のスキャン**: インターネット閲覧するだけで感染する危険がある、ウェブページ経由のウイルスをスキャンします。ユーザーが閲覧しようとしたコンテンツでウイルスを検出すると、そのコンテンツの実行をストップして、コンピュータを感染から守ります。なお、ウイルスが検出された場合、ウェブページは表示されません。この設定を有効にするには、**インターネットコンテンツ（HTTP）のスキャン**にチェックを入れます。

ウェブコンテンツのスキャンを無効にした場合
ウイルスガードは必ず有効にしてください。感染ファイルが実行されると、ウイルスガードがこれを検出します。

特定サイトを例外に設定するには、**例外**の項を参照してください。**「詳細設定」**からインターネットコンテンツ関連の設定を行うことができます。なお、例外設定は、Internet Explorer と Firefox の両ブラウザからは専用プラグイン経由で直接行うことができます。

- **フィッシング保護:** オンラインバンキング、オンラインショップ、ネットオークションの偽造サイトに誘導し、顧客データを盗むフィッシングサイトをブロックします。インターネットを閲覧するときは、フィッシング保護は常時有効にすることをお勧めします。

- **感染したウェブページのアドレスを送信:** プログラムによって危険と判断されたウェブページの情報が G Data に自動的に送信されます。なお、送信元が特定できるようなデータは送信されません。収集されたデータは、すべてのユーザーがインターネットをより安全に利用できるために役立てられます。

- **IM コンテンツの処理（ポート番号入力で Skype も処理可能）**：メッセンジャー経由での感染を防ぎます。アプリケーションがデフォルトのポート番号（5190）を使用していない場合には、**「詳細設定」**を押して、**サーバーポート番号**の欄に適切なポート番号を入力してください。

- **IMアプリケーションへの統合:** Microsoft Messenger **(バージョン4.7以降)** または Trillian **(バージョン3.0以降)** がインストールされている場合は、ここにチェックを入れることにより、疑わしいファイルをすぐにスキャンできるコマンドを右クリックメニューに追加できます。

例外
ウェブサイトを例外として設定するには、次の手順に沿って行います。

1. **「例外」** をクリックします。そうすると、**ウェブ保護用の例外設定**の画面が開きます。

   この画面では、ユーザーが安全と判定して登録したウェブページが表示されます。

2. 例外のウェブサイトを **ウェブ保護用例外**に追加するには、**「新規作成」** をクリックします。入力画面が開くので、URLの欄にウェブページのアドレス（例： www.gdata.co.jp）と、必要に応じて**説明**の欄に登録の理由などを入力します。

3. 「OK」をクリックすると、ウェブページが例外サイトとして追加され、ウェブ保護の対象から外されます。

例外に登録したウェブページの編集や編集は、登録した項目を選択し、編集の場合は**「編集」**を、削除の場合は**「削除」**をクリックします。

詳細設定
詳細設定では、ウェブ保護が監視する**サーバーポート番号**を設定します。デフォルト設定では、通常のインターネット閲覧に使用する 80 が設定されています。

- **ブラウザのタイムアウトを防止**: **インターネットコンテンツ（HTTP）のスキャン**にチェックを入れた場合、ウェブコンテンツをブラウザに表示する前に不正ルーチンのチェックが行われます。この処理はデータ量によっては処理時間がかかり、ブラウザが表示データをすぐに受信できないため、エラーメッセージが表示されることがあります。**ブラウザのタイムアウトを防止**にチェックを入れると、このエラーメッセージが表示されず、コンテンツ全体のチェックが終了するとウェブページが通常どおり表示されるようになります。
- **ダウンロードの容量制限**: 指定した容量を超過したサイズのコンテンツで、**インターネットコンテンツ（HTTP）のスキャン**を中断するように設定します。この容量制限を利用すると、**インターネットコンテンツ（HTTP）のスキャン**によるインターネットの通信速度低下を回避できるます。なお、容量制限した場合は、ウイルスガードは必ず有効にしておいてください。

メールスキャン
メールスキャンは、送受信メールや添付ファイルにウイルスが混在していないかチェックする機能です。メールスキャンで検出した添付ファイルは削除したり、修復したりできます。

> Microsoft Outlook には、専用プラグインがインストールされます。このプラグインは、メールスキャンで設定できる POP3/IMAP ベースの保護を提供し、これにより、Outlook 上でのウイルスチェックがより簡単にできるようになります。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの [ツール] > [フォルダのウイルスをスキャン] を選択します。

受信メール

- **感染した場合**: 感染メールが検出された場合の処理方法を設定します。コンピュータ環境に応じて、最適な設定を選択してください。一般的には、**ウイルス駆除（不可能な場合は添付ファイル / メール本文を削除）**を推奨します。

- **受信メールのスキャン**: インターネット接続中に受信するすべてのメールに対して、ウイルススキャンを実行します。

- **感染メールへのレポート添付**: ウイルスが検出された場合、感染したメールの件名欄に**「ウイルス」**という警告を挿入します。また、メール本文の先頭に**「注意！このメールはウイルスに感染しています」**というメッセージ、ウイルスの名称、ウイルスの駆除または感染ファイルを修復したなどの情報を表示します。

送信メール

- **送信前のメールスキャン**: ウイルス添付メールの外部送信を防ぐために、送信前にメールをチェックします。この機能が有効な場合、ウイルス添付メールを送信しようとすると、**「メール [件名] には次のウイルスがあります: [ウイルス名]」**というメッセージが表示され、メールの送信はブロックされます。

スキャンオプション

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Data には、2 種類の**高性能ウイルス検索エンジン**を搭載し、世界最高レベルのウイルス検出率を実現しています。通常は**2つのエンジン（推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **アウトブレイクシールド**: パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド（OutbreakShield）を有効にします。アウトブレイクシールドは、ウイルスが初めて発見された時点から数十秒から数分内でウイルスメールを検出できます。

詳細設定

メールプログラムに**標準ポート**を割り当てていない場合には、メールの送受信に使用する**ポート**を**サーバーポート番号**の欄に入力してください。**「標準」**をクリックすると、自動的に標準のポート番号にリセットされます。複数のポートをスキャンさせたい場合は、コンマ（ , ）でそれぞれのポート番号を区切って入力してください。

Microsoft Outlook がインストールされているコンピュータでは、専用プラグインが自動的にインストールされます。この Outlook プラグインを使うと、Outlook 上で簡単な操作でメールスキャンができるようになります。スキャンを実行するには、スキャンする対象のメールまたはフォルダを選択し、Outlook のメニューバーから [ツール] > [フォルダのウイルスをスキャン] を選択してください。

受信メールはメールプログラムが実際にメールを受信するより先に処理するため、大量のメールを受信する場合や通信速度が遅い場合には、メールプログラムがエラーメッセージを表示することがあります。原因は、本製品がメール内のウイルスをスキャンして、メールプログラム側でのメール受信による遅延が発生するためです。**メールクライアントのタイムアウトを防止**にチェックを入れると、メールプログラムの前述のエラーが表示されなくなります。本製品がチェックするメールは、スキャンが終了次第、メールプログラムに引き渡されます。

自動ウイルススキャン
ユーザーがコンピュータを使用していない場合に自動的にスキャンが行われるアイドリングスキャン機能を設定したり、スキャン対象、スキャン実行日時や頻度、エンジンの種類などをカスタムしたスケジュールスキャンを設定できます。

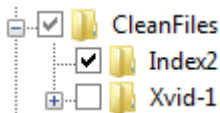
自動ウイルススキャンの設定を作成するには
自動ウイルススキャン領域で、**「新規作成」**をクリックします。ダイアログ画面が開くのでまず名前を入力し、必要な項目を設定してください。例えば、ダウンロードしたファイルを毎日特定の時間にスキャンする場合は、**スキャン範囲**の**次のフォルダとファイルをスキャン**を選択し、**「選択」**ボタンから対象フォルダを選択します。次に **スケジュール**の**実行頻度**で**毎日**を選択、そして時間を設定して、**「OK」**をクリックすれば設定は完了です。

一般
新規作成する自動ウイルススキャンジョブに名前をつけます。

スキャン終了後にコンピュータの電源を切る（ユーザーがログインしていない場合）にチェックを入れると、スキャン後にコンピュータを自動的にシャットダウンします。

実行されるウイルススキャン処理の単位を**ジョブ**と呼びます。

スキャン範囲
ウイルススキャンを実行する対象を設定します。スキャンの対象は、**ローカルのハードディスクドライブ**、**メモリとスタートアップ**、**次のフォルダとファイルをスキャン**から選択できます。

> **次のフォルダとファイルをスキャン**を選択した場合は、**「選択」**をクリックすると対象を指定します。
>
> フォルダのツリー構造で「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。本製品は、チェックが入っているフォルダまたはファイルをすべてスキャンします。スキャンされていないファイルがあるフォルダは、グレーでチェックされています。

スケジュール
ジョブを実行するタイミングを設定します。実行のタイミングは、**実行頻度**と**時間**を組み合わせて設定します。**実行頻度**で**システム起動時**を選択した場合は、**時間**は非表示となります。

- **スケジュール実行後にコンピュータの電源が切れていた場合、次回の起動時にジョブを実行**: コンピュータを起動していなかったため実行できなかったスキャンジョブを、コンピュータの次回起動した時に自動的に実行します。
- **バッテリモードでは実行しない**: ノートパソコン用の設定です。バッテリー駆動時はスキャンジョブを実行せずに、AC電源での駆動時にスキャンジョブを実行します。

スキャン設定
自動ウイルススキャン用のスキャン設定について定義します。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、ウイルスが検出されるとウイルスと感染ファイルについてのログが残されます。最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイブは、**ログを残すのみ**を選択し、検出の度に処理方法をユーザーが選択することをお勧めします。

「詳細設定」からは実行するスキャンの詳細設定を編集したり、確認できます。

- **ファイルの種類**: スキャン対象とするファイルの種類を選択します。

- **ヒューリスティック**: ワクチンに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、感染していないファイルを感染ファイルと判断してしまうケースもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。

- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。

- **システム領域のスキャン**: システム領域をスキャンします。この設定は常に有効にしておいてください。
- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、勝手に高額なインターネット接続を確立したり、閲覧履歴やキーボードへの入力（パスワードなど）を盗みだしたりする恐れがあります。
- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。
- **ログの作成**: ウイルス検出のログを記録します。ログを閲覧するには、起動画面の右上の**「その他」**をクリックし、プルダウンで表示されるメニューからログを選択してください。

ユーザーアカウント
コンピュータがネットワークに接続されている環境で、接続先もスキャン対象とする場合は、接続先へのアクセス権が必要となります。アクセスに必要な**ユーザー名**、**パスワード**、**ドメイン**を入力してください。

アンチスパム

アンチスパムでは、迷惑な広告メールやスパムメールなどへの対策を有効／無効にします。

スパムフィルタ
スパムフィルタは、スパムメールが持つ特長をもとに数値を算出し、スパムメールを効果的にブロックする機能です。スパムフィルタを有効にするには、**スパムフィルタを使用**にチェックを入れます。一方、スパム無効にする場合は、チェックを外します。スパムフィルタの各項目の設定を変更するには、項目をクリックすると表示される画面から行います。

スパムフィルタには、次の項目があります。

- **スパム アウトブレイクシールド**: パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド（OutbreakShield）を有効にします。アウトブレイクシールドは、ウイルスメールが初めて発見された時点から数十秒から数分内でウイルスメールを検出できます。ワクチン更新で検出が間に合わないウイルスにも、ほぼリアルタイムで対処できます。

  プロキシサーバーを使用している環境では、**「インターネット設定」**をクリックし、設定の変更を行ってください。この設定はアウトブレイクシールドが機能しない場合にのみ変更してください。

- **ホワイトリストを使用**: 特定のメールアドレスやドメインから送信されるメールを、スパムとして判定しないように設定できます。ホワイトリストに登録するには、**ホワイトリストを使用**を選択すると表示されるウィンドウ上の**「新規作成」**をクリックし、**送信者アドレス/ドメイン**の欄にスパム判定から除外するメールアドレス（例：newsletter@gdata.co.jp）またはドメイン（例：gdata.co.jp） を入力して、**「OK」**をクリックします。そうすると、入力された送信者またはドメインからのメールを、スパムではないと判定されるようになります。

  また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをホワイトリストに追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。

  「エクスポート」からは、上述のホワイトリストをテキスト形式で書き出します。

- **ブラックリストを使用**: 特定のメールアドレスやドメインから送信されるメールを、スパムとして判定するように設定できます。ブラックリストに登録するには、**ブラックリストを使用**を選択すると表示されるウィンドウ上の**「新規作成」**をクリックし、**送信者アドレス/ドメイン**の欄にスパム判定するメールアドレス（例：newsletter@spam.co.jp）またはドメイン（例：spam.co.jp）を入力して、**「OK」**をクリックします。そうすると、入力された送信者またはドメインからのメールは、自動的にスパムと判定されるようになります。

  また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをブラックリストに追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。

「エクスポート」からは、上述のブラックリストをテキスト形式で書き出します。

- **リアルタイムブラックリストを使用**: スパム送信に使用されているサーバーのブラックリストをもとに、受信メールがスパムメールであるかどうかを確かめます。サーバーがリストに掲載されていれば、スパムの可能性は高くなります。この設定はデフォルト設定のままでの使用をお勧めますが、カスタムも可能です。

- **キーワード（メール本文）を使用**: **メール本文**に使用されている単語をもとに、スパムメールかどうかを判断します。リストの 1 語以上がメール本文に使用されていると、スパムの可能性が高まります。

  キーワードのリストは、**「新規作成」**、**「編集」**、**「削除」**が可能です。また、**「インポート」**をクリックすると、自身で作成した**キーワード**リストを追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。**「エクスポート」**からは、既存のキーワードリストをテキスト形式で書き出します。 **完全なキーワードのみ検索**にチェックを入れると、完全に一致する単語だけを検索します。 例えば「cash」という単語がリストに登録されていても、「Cashew」はスパムと判定されません。

- **キーワード（件名）を使用**: **メールの件名**に使用されている単語をもとに、スパムメールかどうかを判断します。リストの 1 語以上が件名に使用されていると、スパムの可能性が高まります。キーワードの編集は、**キーワード（メール本文を使用）**と同様の操作で行います。

- **コンテンツフィルタを使用**: **コンテンツフィルタ**は自己学習型フィルタで、**メール本文**の単語を基準にしてスパムの可能性を計算します。このフィルタは、変更できない単語リストだけを基準にして機能するのではなく、新着メールが届くたびに学習してリストを拡張していきます。**「テーブルコンテンツを検索」**をクリックすると、メールをスパムに分類するコンテンツフィルタが使用している単語リストを表示できます。**「テーブルをリセット」**をクリックすると学習したテーブルの内容がすべて削除され、自己学習型コンテンツフィルタが学習プロセスを最初からやり直します。

処理方法
スパムの疑いがあるメールの処理方法は、スパム判定された3種類の段階で設定できます。

- **スパムの可能性があるメール**では、スパムの特徴を持つメールが検出された場合の処理ルールを設定します。ここに振り分けられたメールには、受信者が配信を希望するニュースレターが紛れ込むこともあります。そのため、受信者にはスパムの可能性を通知する設定をお勧めします。

- **スパムの可能性が高いメール**では、スパムの要素を多数持っているメールが検出された場合の処理ルールを設定します。この中にはまれに受信者が配信を希望するメールが含まれることもあります。

- **スパムの可能性が非常に高いメール**では、スパムメールの要件をすべて満たすメールが検出された場合の処理ルールを設定します。ここに配信を希望するメールが紛れ込むことはほとんどありません。ここに振り分けられたメールは受信拒否することをお勧めします。

この3 種類の処理方法については、それぞれ独自にカスタマイズできます。変更を行うには、**「変更」** をクリックします。

「変更」を押すと表示される画面内にある**メールを拒否**にチェックを入れると、スパムと判断されたメールを受信トレイに入れません。また、**メールの件名**と**本文にスパム警告を挿入**にチェックを入れると、スパムと判断されたメールに警告を挿入します。Microsoft Outlook を利用している場合は、**メールをフォルダに移動**からスパムの疑いのあるメールを受信フォルダ内の任意のフォルダ（デフォルト設定：アンチスパム）に移動できます。

Microsoft Outlook を使用していない場合でも、スパムと判断されたメールをフォルダに移動できます。メールを移動するには、件名欄に警告 ([Spam] など) を挿入し、使用しているメールプログラムで、警告されたメールを別のフォルダに移動させるルールを作成します。

上級者用設定
スパム検出の基準として使用されるスパムインデックス値を詳細にカスタマイズできる上級者用の設定です。専門知識を必要とする設定のため、通常はデフォルト設定のままで使用する事をお勧めします。

フィルタの追加
デフォルト設定では次のフィルタが有効になっています。

- HTMLスクリプトの無効化
- 有害な添付ファイルのフィルタ

更に新規フィルタをマニュアルで追加したり、既存のフィルタを編集することもできます。作成したフィルタは **フィルタリスト**で一覧表示され、チェックボックスを使って、有効／無効を簡単に切り替えることができます。

新規フィルタを追加するには、**「新規」**をクリックし、表示されたダイアログ画面で**フィルタの種類**を選択して**「OK」**をクリックしてください。続いて選択した**フィルタ**の設定アシスタント画面が開くので、必要な情報を入力して**「OK」**をクリックします。フィルタを削除するには、対象のフィルタを選択して、**「削除」**をクリックします。

- HTMLスクリプトの無効化: このフィルタは、メールのHTML部分のスクリプトを無効にします。HTMLスクリプトは、ウェブページで利用されるスクリプトですが、コンピュータを感染させるために メールに埋め込まれて悪用されることがあります。

- **有害な添付ファイルのフィルタ**: メールに添付されている危険な添付ファイルをフィルタします。多くのメールウイルスは、EXEファイルや画像（動画または音楽）ファイルに仕掛けられたVBスクリプトや隠し実行ファイルが含まれる添付ファイルを通して広がります。メールの添付ファイルを実行する際は、十分に注意してください。場合によっては、送信者に確認するのも感染から有効な手段の１つです。

  ファイル拡張子では、フィルタに適応する拡張子を指定します。指定できる拡張子の種類は、実行ファイル（EXEファイルやCOMファイルなど）の他、画像／動画／音楽ファイル（MPEG／AVI／MP3／JPEGなど）や圧縮ファイル（ZIP／RAR／CABなど）の拡張子もフィルタできます。複数の拡張子を指定する際は、それぞれの拡張子をコンマ（,）で区切ります。

  添付ファイルのみ名前を変更にチェックを入れると、フィルタする添付ファイルは自動削除されずに、ファイル名が変更されます。ファイル名を変更すると、実行ファイルや実行可能なスクリプトやマクロを含むMicrosoft Office 形式のファイルをクリックしただけでは実行できないので、誤ってクリックしての感染などを未然に防ぐことができます。ファイル名が変更されたファイルを実行するには、ユーザーはファイルを任意の場所に保存し、本製品によって付与された拡張子（デフォルト設定では_danger）を消去する必要があります。危険とみなされたファイルに付与する拡張子はユーザーが自由に設定できます。**添付ファイルのみ名前を変更**にチェックを入れない場合は、フィルタされたファイルはすぐに削除されます。

  メール本文にメッセージを挿入にチェックを入れると、危険な添付ファイルが含まれていた場合、判断されたメールにテキストを挿入し、添付ファイルが削除された（もしくは名前が変更された）ことをユーザーに知らせます。

- **コンテンツフィルタ**: コンテンツフィルタは、特定のテーマまたはテキストを含むメールの受信をブロックします。コンテンツフィルタを設定するには、まず**検索基準**に、フィルタするキーワードと表現を入力します。論理演算子 AND および OR を使うと、キーワードや表現を複数入力できます。

  検索範囲では、メールのどの部分でこの表現を検索するかを指定します。**ヘッダ**では、送信者および受信者のメールアドレス、件名、メールプログラムの情報、プロトコル、送信者情報がフィルタの対象となります。**件名**では、件名欄の内容だけをチェックします。

  メール本文では純粋なテキストメール 、**HTML テキスト**ではHTMLメールをチェックします。**埋め込みメール**では、コンテンツフィルタの対象を受信メールの本文に添付ファイルが埋め込まれているメールをフィルタ対象とするかどうかを指定します。

  処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に**「スパム」**または**「注意」**などの警告（**[件名に追加する文字]**）を挿入できます。

  メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合には、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます（**[本文中のメッセージ]**）。

  Microsoft Outlook （※Outlook Express や Windows Mail では不可）を使用している場合 、スパムの疑いのあるメールを受信トレイ内の任意のフォルダに移動できます （**[メールをフォルダに移動]**）。移動先のフォルダは、**フォルダ名**に入力すると新規作成できます。

- **送信者フィルタ**: 送信者フィルタは、特定の送信者から送られてきたメールの受信をブロックします。送信者フィルタを設定するには、**送信者 / ドメイン**に、ブロックする送信者のメールアドレス とドメイン名 を入力します。複数の送信者を登録する場合には、メールアドレスをセミコロン (;) で区切ります。

  処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」または「注意」などの警告（件名に追加する文字）を挿入できます。

  メールを拒否 を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます（**本文中のメッセージ**）。

  Microsoft Outlook を使用している場合（※Outlook Express または Windows Mail では不可）、スパム疑惑のあるメールを受信トレイ内の自由に定義できるフォルダに移動することができます（**メールをフォルダに移動**）。本製品は、**フォルダ名**の欄にフォルダを定義すれば直接フォルダを作成する機能を備えています。

- **言語フィルタ**: 言語フィルタでは、特定の言語で書かれたメールをスパムとして定義します。例えば、英語のメールを受信することはないという場合には、英語をスパム言語として定義し、多数の英語で送られてくるメールを排除できます。メールを受け取ることはない言語と考えられる言語を選択すると、スパム検出精度はさらに向上します。

  処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」または「注意」などの警告**（件名に追加する文字）**を挿入できます。

  「メールを拒否」 を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます**（本文中のメッセージ）**。

  Microsoft Outlook を使用している場合（※Outlook Express または Windows Mail では不可）、スパムの疑いのあるメールを受信トレイ内の自由に定義できるフォルダに移動することができます**（メールをフォルダに移動）**。本製品は、**フォルダ名**の欄にフォルダを定義すれば直接フォルダを作成する機能を備えています。

その他
ここでは次の設定を行うことができます。

- **プログラム起動時に受信トレイの未読メールをスキャン**（Microsoft Outlook のみ）: Outlook を起動するとすぐに、受信トレイとそのサブフォルダにあるすべての未読メールをチェックします。
- **他のメールプログラム（POP3 を使用)**: POP3 で受信したメールは、POP3による技術的な理由で、すぐには削除できないことがあります。フィルタがメールの受信を拒否すると、このメールは下の代替テキストで書き換えられます。受信拒否メールの代替テキストは**「メッセージが拒否されました」**と表示されます。この代替テキストは自由に編集できます。件名とメール本文のテキストを、以下のワイルドカード (「%」記号に続けて小文字 1 文字) を使って自由に作成できます。

%s	送信者
%u	件名

ここで設定したテキストを自動的に削除するルールをメールプログラムで設定できます。

ファイアウォール

ファイアウォールは外部からの不正侵入からコンピュータを保護します。G Data のファイアウォールには、オートパイロットモードからマニュアルでのルール設定まで、初心者から上級者のニーズに応えることができる様々な設定が搭載されています。

ファイアウォールに関する詳細は、**ファイアウォールの操作**を参照してください。

自動

ファイアウォール設定の**自動**は、以下の2つの領域から構成されています。

自動

ファイアウォールの作動方式を選択します。モードでは、**オートパイロットモード（推奨）**と**手動でルールを作成**から選択できます。

- **オートパイロットモード**: ファイアウォールが許可、またはブロックするアプリケーションを自動制御するので、ユーザーを煩わすことなく、コンピュータを最適に保護できます。（推奨設定）
- **手動でルールを作成**: ファイアウォールをネットワーク環境に合わせて設定したり、特定のアプリケーションにオートパイロットモードを適用しない場合には、この設定を選択して、ルールを手動で作成します。
- **フルスクリーンアプリケーション実行時にオートパイロットを実行（ゲームモード）**：ゲームやフルスクリーン表示のアプリケーションを起動した際に、ファイアウォールが自動的にオートパイロットモードに切り替わるように設定します。この設定は、オートパイロットを通常は使用しない場合にのみ選択できます。

自動セキュリティレベル

上級者向けの**ユーザー定義セキュリティ （上級者向け）**と G Data が定義した**自動セキュリティレベル**から選択できます。**自動セキュリティレベル**を使用すると、ネットワークセキュリティの専門知識がなくてもユーザーを煩わせることなく、ファイアウォールを環境に応じて設定できます。**自動セキュリティレベル**の設定は、非常にシンプルで、希望するセキュリティレベルにスライダを合わせて設定するだけです。設定レベルには以下の5種類があります。

- **最高セキュリティ**: ファイアウォールのルールを非常に細かく設定します。ネットワークの専門用語（TCP、UDP、ポートなど）に精通している必要があります。ファイアウォールは微小な不一致も検知するため、学習段階では非常に頻繁に確認が行われます。

- **高セキュリティ**: ファイアウォールのルールを細かに設定します。ネットワークの専門用語（TCP、UDP、ポートなど）に精通している必要があります。ファイアウォールが、学習段階で頻繁に確認が行われます。

- **標準セキュリティ**: ファイアウォールのルールをアプリケーションレベルで設定します。ネットワークの専門知識がなくても、ウィザードで簡単に設定できます。学習段階での確認頻度も最小限です。

- **低セキュリティ**: ファイアウォールのルールをアプリケーションレベルで設定します。ネットワークの専門知識がなくてもウィザードで簡単に設定できます。また、学習段階での確認もほとんどありません。このセキュリティレベルでも、着信する接続要求に対しては最高レベルのセキュリティが適用されます。

- **ファイアウォール無効**: ファイアウォールを無効にします。ファイアウォールを無効にしても、インターネットや他のネットワークとの接続は維持されます。外部からの攻撃やスパイウェアの防御が機能しなくなるので、ファイアウォールを無効にする際は注意ください。

ファイアウォールを細かく設定するには、**ユーザー定義セキュリティ（上級者向け）**にチェックを入れます。この設定は、ネットワーク知識のある上級者にのみお勧めします。

アラート
プログラムがインターネットやネットワークと接続を確立する時に、ファイアウォールがユーザーに確認を求めるタイミング、処理方法、確認の有無などを設定します。

- **ルールの作成**: ファイアウォールがネットワークとの接続を確立すると、ポップアップが表示され、当該アプリケーションを許可／禁止するなどの処理方法を指定します。

  アプリケーションごと: 表示されているアプリケーションに対して、許可／拒否するポートおよびプロトコルを設定します。

  プロトコル/ポート/アプリケーション: ネットワーク接続を要求するアプリケーションに、要求されたポート（またはプロトコル）だけを使用したアクセスを許可します。このアプリケーションがさらに別のポート（またはプロトコル）でネットワーク接続を要求した場合は、追加ルールを作成するために、再びユーザーに確認が行われます。

  アラートの保留数を指定　__ アラートまで保留: 一部のアプリケーション（Microsoft Outlook など）は、複数のポートやプロトコルを使用しています。**プロトコル / ポート / アプリケーションごと**の設定下で、このようなアプリケーションを使用しているケースでは、ユーザーへの確認が複数回行われますが、特定回数以上、ユーザーへの確認があった場合は、**アプリケーションごと**に切換え、当該アプリケーションに対して許可／拒否を行うことができます。

- **不明なサーバーアプリケーション**: ファイアウォールのルールにないサーバーアプリケーションが起動した場合、もしくはコンピュータが、ファイアウォールのルールにないサーバーアプリケーションから接続を受けている状態（例： ポート開放）に入った時に、ファイアウォールに報告させる事ができます。

- **保護されていないワイヤレスネットワーク**: ファイアウォールが適切に機能するには、コンピュータが接続しているネットワークが認識され、かつファイアウォールによって監視されている必要があります。このため、通常はデフォルト設定の**保護されていないワイヤレスネットワークが発見されたらすぐに警告する**からはチェックを外さないでください。

- **アプリケーションアラートのキャッシュ**: ファイアウォールのルールで定義されていない接続要求において、繰り返し行われる接続確認を特定の間隔で行うように設定できます。デフォルトでは、20秒に設定されています。

チェックサムテスト
チェックサムテストでは、ファイアウォールによってネットワークへのアクセスを許可されたアプリケーションに対し、ファイル容量などの判断基準から構成されるチェックサムを使い、その信頼性をチェックします。アプリケーションのチェックサムが一致しない時は、アプリケーションが改変された可能性があるので、ファイアウォールはアラートを表示します。

チェックサムテストの実行では、アプリケーションが使用するモジュール（例：DLL）を監視します。モジュール変更や新たなモジュールのロードは頻繁に行われるため、モジュール変更と不明なモジュールを完璧に管理するのは非常に手間がかかります。モジュールチェック機能は非常に高レベルのセキュリティが必要な場合にのみ使用してください。

その他
次のようなファイアウォールに関する設定が可能です。

- **デフォルト設定ウィザード**: 新規ルールの生成方法をルールウィザードもしくは詳細設定ダイアログから選択します。**詳細設定ダイアログ**は上級者向けの設定モードです。
- **プログラム起動時のチェック**: ファイアウォールがアプリケーション起動するごとに不明なサーバーアプリケーションをチェックします。この設定は、クローズドネットワークを除くすべてのネットワーク環境で有効にしておく事をお勧めします。
- **接続ログの保存**: ファイアウォールの接続ログデータを保管する期間を設定します。期間は1～60時間の中から選択できます。ファイアウォールのログは、ファイアウォールを開いて、画面左下に配置されているログから確認できます。

ファイアウォールの操作

ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インターネットやネットワークとコンピュータとの間で送受信されるデータを監視します。

ステータス

ステータスでは、ファイアウォールの状態に関する基本情報が項目ごとに表示されます。項目をダブルクリック（または選択して **「編集」** をクリック）すると、関連領域に切り替わります。

警告マークの付いた項目の設定が最適化されると、ステータス領域のこのマークは再び緑色のチェックマークに戻ります。

- **セキュリティ**: ファイアウォールは、インターネットに接続したり、コンピュータに悪影響を及ぼすアプリケーションを自己学習していきます。ファイアウォールに関する知識の程度に応じてファイアウォールの構成を変えることができます。ユーザーへの確認の頻度を減らしてもセキュリティレベルの高い基礎的保護がなされるように設定することもできれば、コンピュータの使用状況に合わせた高水準の保護が得られるように詳細設定することも可能です。ただし、詳細設定を利用は、上級者のみにお勧めします。**セキュリティ**をダブルクリックして、以下のようなセキュリティモードを選択できます。

- **モード**: 作動中のファイアウォール設定を確認できます。設定は、**オートパイロットモード（推奨）**と**手動でルールを作成** のいずれかから選択できます。

  オートパイロットモード（推奨）: ファイアウォールがアプリケーションの許可／ブロックを自動判断で制御し、コンピュータを保護します。（推奨設定）

  手動でルールを作成: ファイアウォールをネットワーク環境に合わせて設定する場合、あるいは特定のアプリケーションにオートパイロットモードを適用しない場合には、ルールを手動で作成できます。

- **ネットワーク**: ファイアウォールが監視中のすべてのネットワークを表示します。手動でファイアウォールを解除した場合など、ネットワークが保護されていない場合には警告マークが表示されます。警告マークが表示された**ネットワーク**の上でダブルクリックすると、ネットワーク領域に移動します。保護されていないネットワークでファイアウォールを有効にするには、ネットワーク領域で表示された一覧から対象を選択してダブルクリック（もしくは「編集」ボタンをクリック）してください。ダイアログ画面が開き、選択したネットワークの使用環境に合わせたルール作成や設定の変更ができます。**ルールセット**の欄で、ネットワークを**信頼性の高いネットワーク**、**信頼性の低いネットワーク**、**アクセスを拒否するネットワーク** などに分類できます。

  ネットワークには、それぞれ独自のルールセットを割り当てることができます。ファイアウォールの**ネットワーク**領域ではすべてのネットワークが表示されます。また、ルールセット領域では、デフォルトとカスタム作成したすべてのルールセットが表示されます。

- **メッセージ**: コンピュータへの攻撃が検知されると、ファイアウォールはこれをブロックし、ログとして記録します。この項目の上でクリックすると、ブロックした攻撃に関する詳細な情報を見ることができます。
- **アプリケーションレーダー**: アプリケーションレーダーは、その時にファイアウォールが起動をブロックしているプログラムを表示します。ブロックされたアプリケーションのうちネットワーク使用を許可したいものがあれば、そのアプリケーションを選択して **「許可]** をクリックします。

ネットワーク

ネットワークでは、コンピュータが接続しているネットワーク （LAN接続、DTN （ダイヤルアップ接続）など）の一覧、適応されているルールセット、IPアドレスが表示されます。

ネットワークからチェックを外すと、そのネットワークに対するファイアウォールによる保護が解除されます。※特別な理由がない限り、ファイアウォールの保護は解除しないようにしてください。

表示されている設定を確認したり、編集したりするには、対象を選択してダブルクリック（もしくは対象を選択して**「編集」**をクリック）します。

編集
ネットワーク設定を編集するには、ルールウィザード もしくは 詳細設定ダイアログ のいずれかを使用します。通常はルールウィザードの使用をお勧めします。ルールウィザードでは、簡単にルールを作成したり、設定できます。

- **ネットワークについて**: IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS および WINS サーバーなどのネットワークに関する情報がある場合、それらを表示します。
- **このネットワークでファイアウォールを有効にする**: ネットワークに対してファイアウォールを無効にできます。特別な理由がない限り、有効にしておいてください。
- **インターネット接続共有**: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定します。このインターネット接続共有（ICS）は通常、ホームネットワークでのみ有効にできます。
- **自動設定を有効にする（DHCP）**: DHCP（Dynamic Host Configuration Protocol）を使用したネットワークでは、コンピュータを接続すると動的に IP アドレスが割り当てられます。このネットワークに接続している場合は、設定を有効にしてください。
- **ルールセット**: **信頼性が高い**、**信頼性が低い**、または**アクセスを拒否する**ネットワークという複数のルールセットから選択し、ファイアウォールルールを素早く設定できます。さらに**「編集」**をクリックすると、これらのルールセットを編集して独自のルールを作ることもできます。詳細ついては、ルールセットを参照してください。

ルールセット

ファイアウォールの細かいルール郡から構成されているルールのまとまりをルールセットといいます。ルールセット領域では、それぞれのネットワークに応じた固有のルールを作成できます。作成されたルールセットは、ルールセット領域にすべて表示されます。

本製品にプリセットされているルールセットには、**アクセスを拒否するネットワーク**、**インターネットに直接接続**、**信頼性の低いネットワーク**、**信頼性の高いネットワーク**があります。それぞれのルールセットの内容を確認や修正するには、ルールセットを選択して**「編集」**を押します。新規ルールを作成するには、**「新規作成」**のボタンを押し、ダイアログに沿ってルールを作成してください。

ユーザーによって作成されたルールセットは削除できますが、本製品に前もって設定されているルールセットは削除できません。

新規作成

ネットワークごとに異なる設定のルールセットを割り当てる事で、ファイアウォールは様々なセキュリティレベルのネットワークに対応できます。

ルールセットを新規作成する場合は、次の３種類のネットワーク用のルールセットが利用できます。

- **信頼性の低いネットワーク用のルールセット**: ダイヤルアップネットワークやその他のインターネット接続するオープンネットワーク用のルールセットです。
- **信頼性の高いネットワーク用のルールセット**: ホームネットワークや企業ネットワーク などの信頼できるネットワーク用のルールセットです。
- **アクセスを拒否するネットワーク用のルールセット**: あるネットワークへの接続を一時的または常時ブロックします。この設定は、セキュリティのレベルが不明なネットワーク （例: 他社の企業ネットワーク、公共ネットワークなど）に接続する時に適用してください。

コンピュータで新規ネットワークを作成した場合は、そのネットワークに適用するルールセットを割り当てるか、**「新規作成」**から新しいルールセットを作成して適用してください。ルールセットを新規作成するには、ルールセット領域で**「新規作成」**をクリックすると表示されるダイアログで、次の項目を定義して設定します。

- **ルールセット名**: ルールセットの名前を入力します。
- **空のルールセットを生成**: 空のルールセットを作成しておいて、ルールを自身で定義して追加します。
- **推奨ルールを含むルールセットを生成**: G Data のプリセットルールの**信頼性の高いネットワーク**、**信頼性の低いネットワーク**、**アクセスを拒否するネットワーク**から選択してルールを作成します。作成されたルールセットは、必要に応じて後からカスタムできます。

新規作成されたルールセットは、ルールセット領域に表示されます。作成したルールセットを変更するには、マウスで選択して**「編集」**を押してください。**ファイアウォール > 設定 > その他** の**デフォルト設定ウィザード**で定義されている設定でファイアウォールを編集できます。

新規ルールセットの作成方法は、**ルールウィザードを使用**もしくは**詳細設定ダイアログを使用 （上級者用）**の項を参照してください。

新規ルールは、ポップアップで表示されるアラートからも作成できます。詳細は**アラート**の項を参照してください。

ルールウィザードを使用

ルールウィザードは、既存のルールセットに特定のルールを追加したり、既存のルールを編集する際に、ユーザーをサポートするウィザード形式の設定アシスタントです。ファイアウォール上級者以外は、**詳細設定ダイアログ**より**ルールウィザード**を利用することをお勧めします。

ルールアシスタントを使用すると、選択したルールセットに含まれるルールを簡単に編集できます。
ネットワークに適用したルールセットの種類によって、アプリケーションは遮断されたり、許可されたりします。例えば、ホームネットワークでネットワーク接続を許可する一方で、ダイヤルアップ接続では拒否するといった設定も可能です。

ルールウィザードでは次の基礎ルールを選択できます。

- **アプリケーションへのアクセスを許可/拒否**: インストールされているアプリケーションを選択し、ルールセットで指定したネットワークへのアクセスを許可／拒否します。目的のアプリケーションのある場所を示す文字列（パス）を選択して、**接続の方向**でそのプログラムにインバウンド接続（着信接続）、アウトバウンド接続（発信接続）のどちらを許可するか、あるいはイン／アウトバウンド接続の両方を許可するかどうかを設定します。例えば、音楽再生ソフトの場合では、次のような利用ができます。

  アウトバウンド接続を拒否して、ユーザーの音楽嗜好データを自動送信するのを防止
  インバウンド接続を拒否して、プログラムの自動更新を遮断

- **インターネットサービス（ポート）を開放/遮断**: **ポート**とは、外部とデータを入出力するため、アプリケーションによって使用されるネットワークアドレスの一部です。例えば、ウェブページの閲覧ではポート80、メール送信にはポート25、メールの受信にはポート110が割り当てられています。ファイアウォールを使用しない場合には、すべてのポートが開放状態になっているので、外部の第三者から攻撃を仕掛けられる可能性があります。ルールウィザードを使用すると、特定のアプリケーションに必要なポートのみ許可し、その他のポートは遮断します。

- **ファイルおよびプリンタ共有（NetBIOS）を許可/拒否**: NetBIOSとはLANでネットワークを利用する際の通信規約で、TCP/IP プロトコルなどを使用せずに、コンピュータ間で直接ファイルやプリンタを共有するのに利用されています。これは、一般的なホームネットワークではほぼ不要ですが、ハッカーが NetBIOS を使ってコンピュータを攻撃する可能性もあるので、信頼性の低いネットワークに対しては共有を拒否してください。

- **ドメインサービスを許可/拒否**: ドメインはあるネットワーク内にあるコンピュータを整理して一覧できるようにするためのもので、ネットワークに接続しているコンピュータを 1 か所で管理できるように割り当てられています。ドメインサービスを許可（もしくは拒否）します。信頼できないネットワークでのドメインサービスの共有は拒否してください。

- **インターネット接続共有を許可**: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定します。このインターネット接続共有（ICS）は通常、ホームネットワークでのみ有効にできます。

- **VPN接続を許可/拒否**: VPN接続を利用している場合、ここで許可／拒否の設定をできます。

- **詳細設定ダイアログへ切換え（上級者用）**：ファイアウォールのデフォルト設定ウィザード（ルールセットの作成モード）を詳細設定ダイアログへ切換えます。

今後もルールウィザードを起動からチェックを外すと、ファイアウォールは新規ルールに対して自動的に詳細設定ダイアログを開くようになります。

詳細設定ダイアログを使用
ネットワークセキュリティに関してある程度の知識があるユーザーは、詳細設定ダイアログを使ってルールセットを更に詳細に設定できます。詳細設定ダイアログでは次の設定ができます。

- **名前**: 選択したルールセットの名前を変更できます。ルールセットはこの名前でルールセット領域に表示され、ファイアウォールが識別したネットワークに結び付けられます。
- **ステルスモード**: コンピュータで使用しているポートの確認に対して応答せず、情報を外部に漏らしません。
- **ルールにないアクセスが検知された場合の操作**: ネットワークのアクセスをすべて許可／拒否するか、あるいはユーザーへの確認で決めるかを設定できます。ファイアウォールの学習機能で個々のアプリケーションに専用ルールを設定している場合は、そのルールが適用されます。
- **アダプティブモード**: フィードバックチャネル技術を使用するアプリケーション（FTPや各種オンラインゲームなど）をサポートします。この種のアプリケーションはリモートコンピュータに一旦接続し、その後、リモートコンピュータがユーザーのアプリケーションに「逆接続」するフィードバックチャネルを確保します。アダプティブモードを有効にしておくと、ファイアウォールがこのフィードバックチャネルを検出するため、特に確認を求められることなく接続を許可できます。

ルール
ルールでは、ルールセットに含まれるに細かなルールが登録されています。ルールセットは以下の3種類の方式で作成されます。

- ルールウィザード
- 詳細設定ダイアログ
- アラート

作成されたルールセットには、それぞれ独自のルールが含まれています。

> ファイアウォールルールは、一部が階層構造でまとめられているため、場合によってはルールの**ランク順**に注意する必要があります。例えば、ポートを開放しているにもかかわらず、そのポートを利用しているアプリケーションが遮断される可能性があります。このような場合は、ルールのランク順を変更するとアクセスが許可されるようになります。ランク順を変更するには、目的のルールをマウスで選択して**ランク**の欄の矢印ボタンでリストの上位または下位へ移動してください。

詳細設定ダイアログで**「新規作成」**から新規ルールを作成したり、**「編集」**ボタンから既存ルールを変更すると、**ルールを編集**ダイアログが表示されます。このダイアログでは、以下の項目を設定できます。

- **名前**: デフォルトルールおよび自動的に作成されたルールの場合、アプリケーション名が入ります。名前は自由に変更できます。
- **有効なルール**: ルールの有効／無効を切り替えます。ルールを無効にするには、チェックを外します。ルール自体を削除する必要はありません。
- **コメント**: ルールを作成した方法が表示されます。ルールセットに対するデフォルトルールには**デフォルトルール**、アラートから作成したルールには**アラートにより作成**と自動的に入力され、ユーザーが詳細設定ダイアログで作成したルールの場合にはユーザーが自分でコメントを入力できます。
- **接続の方向**: ルールをインバウンド接続（着信接続）とアウトバウンド接続（発信接続）のどちらに適用するかを指定します。
- **アクセス**: ルールセット内で各プログラムに対してアクセスを許可するかどうかを設定します。

- **プロトコル**: アクセスを許可または禁止する接続プロトコル を選択できます。このとき、プロトコルを原則として停止または許可する、またはプロトコルの使用を 1 つのアプリケーションまたは複数のアプリケーションと組み合わせる（アプリケーション割当て）ことができます。同様に、許可するポートとブロックするポートを**「インターネットサービス割当て」**から厳密に定義できます。

- **時間**: ネットワークリソースへのアクセス時間を設定できます。これにより、アクセス許可を業務時間内に限定して、それ以外の時間はアクセスできないように設定できます。

- **IP アドレス範囲**: 固定 IP アドレスを持ったネットワークでは、IP アドレス範囲を限定して使用方法も可能です。IP アドレス範囲を厳密に定義すれば、ハッカーから攻撃を受ける危険性を大幅に低減できます。

アラート

手動でルールを作成モードでは、未知のアプリケーションやプロセスがネットワークへのアクセスを試みると、アクセスの許可／拒否について、ユーザーに確認が行われます。

確認は、画面の右下からのポップアップで行われます。このポップアップでは、ユーザーは、アプリケーションに対して、ネットワークアクセスを**一時的に許可/拒否**または**常に許可/拒否**という処理方法から選択できます。アプリケーションにアクセスを**常に許可/拒否**すると、操作がアクセスするネットワークのルールセットに取り込まれ、以降はアラートが表示されなくなります。

> ネットワークのルールセットに取り込まれたルールは、**ルールセットのコメント**で**アラートにより作成**と表示されます。

この他にも、アラートのポップアップ画面では、**アプリケーション**や**起動元の詳細表示**、**ネットワーク**の種類、**プロトコル**、**ポート**、**IP アドレス**に関する情報を確認できます。

アラートのポップアップ画面からは、次の選択操作が可能です。

- **常に許可**: アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへのアクセスを常に許可します。ルールセット領域には、アラート経由で作成されたルールとして表示されます。
- **一時的に許可**: アプリケーションに対して、ネットワークアクセスを 1 回だけ許可します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。
- **常に拒否**: アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへの接続を常に拒否します。ルールセット領域には、アラート経由で作成されたルールとして表示されます。
- **一時的に拒否**: アプリリーションに対して、ネットワークアクセスを 1 回だけ拒否します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。

ログ

ログ領域には、ファイアウォールで許可および拒否されたネットワーク接続とインターネット接続がすべて記録されます。

任意の列見出しをクリックすると、その項目に従って並び替えができます。また、行を選択して**「詳細」**をクリックすると、その接続について詳しい情報を表示できます。

フィルタリングの操作

フィルタリングは、こどもを有害コンテンツから保護する目的で、インターネット上のサイトを一定の基準で評価判別し選択的に排除したり、コンピュータの利用時間に制限をかける機能です。フィルタリングの操作は、画面左側の領域の項目から選択し、右側の領域で操作の実行、設定の変更などをを行います。

フィルタリングは、デフォルトのインストールではインストールされません。フィルタリングを追加するには、製品CDもしくはセットアップからインストールウィザードを起動し、ウィザードに従って機能を追加してください。

画面右上のアイコンからは、フィルタリングのテストや設定ができます。

テスト: 管理者としてログインしている状態で、選択したユーザーのフィルタリングが正常に機能するかどうかを、テストできます。この機能は、管理者のみが利用できる機能で、**テストの設定**ダイアログが表示されている間、利用できます。**「テストを終了」**を押すと、フィルタリングのテストを終了します。

設定: フィルタリングのログに関する設定を変更したり、設定内容を確認できます。

ステータス

コンピュータの管理者権限を持つアカウントを持つユーザーであれば、**ユーザー**から特定ユーザーの設定を確認したり、変更したりできます。さらに、ここから Windows の新規ユーザーアカウントを追加することもできます。

コンピュータ上に **Windows ユーザーアカウント**を持つユーザーであれば、**ユーザー**でアカウントが表示されるので、そこから直接選択できます。ユーザーのフィルタリング設定を変更するには、目的のユーザーを選択して**「編集」**をクリックします。

新規ユーザーの作成
「新規ユーザー」をクリックします。ダイアログが開くので、ユーザー名とパスワードを入力します。

> 安全のため、**パスワード**は、『8文字以上（大文字と小文字、数字含まれる）』で構成するようにしてください。

Windows ユーザーアカウントが作成され、ステータス領域の**ユーザー**に新しく追加したユーザー名が表示されるようになります。Windows起動時に作成したユーザー名でログインすると、そのユーザー用に設定したフィルタリングの設定が有効になります。ユーザー用のフィルタリング設定を変更したり確認するには、**禁止するコンテンツ**、**許可するコンテンツ**、**インターネット利用時間の監視**、**コンピュータ利用時間の監視**上でダブルクリックしてください。

禁止するコンテンツ
ダイアログ画面で、ユーザーの禁止するコンテンツを設定します。禁止するコンテンツを有効にするには、禁止したいカテゴリにチェックを入れます。
「OK」をクリックすると、**禁止する基準** を満たすウェブサイトを表示できなくなります。

「新規作成」をクリックするとダイアログ画面が開き、**禁止するコンテンツ**をカスタムで作成できます。禁止コンテンツを作成するには、**パーソナルフィルタを作成**の画面で、**名前**の欄に入力し、ユーザーごとにフィルタを作成している場合には**情報**欄にも入力して、**「OK」**をクリックしてください。

「OK」をクリックすると、次に**禁止するコンテンツの編集**の画面が開くので、**フィルタ**の欄に表示を禁止するキーワードを入力し、**場所を検索**ではキーワードを検索する範囲を入力します。

以下の構成部分から選択します。

- URL: ウェブアドレス内の文字列を検索します。例えば、www.chatcity.co.jp、www.crazychat.co.jp などのサイトを禁止したい場合、フィルタに 「chat」 と入力し、URLにチェックを入れて**「追加」**をクリックします。この設定が有効になると、URLに 「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

- **タイトル**: ウェブサイトのタイトルの文字列を検索します。ここでいうタイトルとは、ウェブページを**ブックマーク**に追加する時に表示されるウェブサイトに付与されている名前です。例えば、Chat City Japan、Teenage Chat などのサイトを禁止したい場合、フィルタに 「chat」 と入力し、**タイトル**にチェックを入れて**「追加」**をクリックします。この設定が有効になると、**タイトル**に 「chat」 という文字列を使用しているページはすべて閲覧できなくなります。

- **メタ**: **メタタグ**（検索エンジンによる検索結果を上げるために利用されるタグです））に記載されている文字列を検索します。例えば、メタタグ内のどこかに文字列「chat」が記述されているページを閲覧禁止にするには、**フィルタ**に「chat」と入力し、**メタ**にチェックを入れて**「追加」**をクリックします。この設定が有効になると、メタタグ内に 「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

- **本文**: ウェブサイト内の本文中の文字列を検索します。例えば、「chat」という文字列が含まれているウェブページをブロックするには、フィルタに「chat」と入力し、次に**本文**にチェックを入れて、**「追加」**をクリックします。この設定が有効になると、本文内に 「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

なお、通常利用されるキーワードを**フィルタ**に設定すると、無害なウェブページを閲覧できなくなることもあります。例えば、禁止キーワードに「cash」を登録すると、「Cashew」という文字列を含むウェブページの閲覧も禁止されかねません。

フィルタに引っ掛かりやすいウェブページを許可するには、**例外**機能を使って例外扱いします。例外を追加するには、まず作成したブラックリストを選択し、**「例外」**をクリックします。**例外リスト**の画面が開くので、上述の例であれば、「Cashew」をフィルタに入力して、**「追加」**をクリックします。

禁止するコンテンツで追加したフィルタは、**パーソナルフィルタ**領域では、**ブラックリスト**（フィルタの種類）と表示されます。作成済みフィルタは、自由に編集したり削除できます。詳細については、**パーソナルフィルタ**の項を参照してください。

許可するコンテンツ
ダイアログ画面で、ユーザーの許可するコンテンツを設定します。許可するコンテンツを有効にするには、許可したいカテゴリにチェックを入れます。
「OK」をクリックすると、**許可するコンテンツの編集**で設定したウェブサイトの表示を許可します。

「新規作成」をクリックすると、**パーソナルフィルタを作成**のダイアログ画面が開くので、**名前**欄に入力（ユーザーごとにフィルタを作成している場合には、**情報**欄にも入力）して、**「OK」**をクリックしてください。

次に、**許可するコンテンツの編集**のダイアログ画面が表示されるので、**フィルタ**の欄に許可する**ドメイン名の一部**を入力します。（例： Kodomo）。**説明**の欄には、ウェブページの内容 （前述の例の場合、「Kodomo: 子供向けウェブページ」など）を入力します。**サイトへのリンク**の欄には、ウェブサイトの正確なアドレス（例: www.kodomo.co.jp）を入力します。**説明**と**サイトへのリンク**に情報を入力すると、ユーザーが禁止されたサイトにアクセスしようとした場合に、許可するリストに登録されたウェブサイトがブラウザ上に表示されます。すべての情報を入力して**「追加」**をクリックすると、情報が許可するコンテンツに登録されます。

> 許可するコンテンツで登録したフィルタは、**パーソナルフィルタ**領域では、**ホワイトリスト**（フィルタの種類）と表示されます。作成済みフィルタは、自由に編集したり削除できます。詳細については、**パーソナルフィルタ**の項を参照してください。

インターネット利用時間の監視
ユーザーのインターネット利用時間を設定します。まずは、ステータス領域でユーザーを選択し、次に**インターネット利用時間の監視**をダブルクリックします。**インターネット利用時間**の設定画面が現れるので、そこで**インターネット利用時間を監視**にチェックを入れます。許可する時間は、月次、週次、曜日ごとに設定できます。許可する時間は、**日 / 時 : 分** の欄に入力するか、マウスを使ってバーをスライドさせて設定します。例えば、**「04 / 20 : 05」** と入力すると、インターネットの利用時間は「4 日間、20 時間と 5 分」となります。

> インターネット利用時間の設定では、常に最小値が適用されます。例えば、1 か月の時間制限を 4 日間と設定する一方で 1 週間の時間制限を 5 日間と設定した場合、ソフトウェアはこのユーザーのインターネット利用時間を自動的に 4 日間に制限します。

ユーザーが許可された制限時間を超えてインターネットにアクセスしようとすると、ブラウザに利用制限時間を超過したことを知らせるメッセージが表示されます。

禁止する時間

「禁止する時間」をクリックしてダイアログを呼び出し、インターネットにアクセスできる時間数の量的制限に加えて、週のうちの特定の時間帯にインターネットにアクセスできないようにできます。

禁止する時間帯は赤色、許可する時間帯は緑色で表示されます。 許可または禁止する時間を指定するには、マウスで時間帯を選択し、マウスポインタの横に表示されるコンテキストメニューで**許可する時間**もしくは**禁止する時間**のいずれかを選択します。ユーザーが禁止時間にインターネットにアクセスしようとすると、ブラウザに利用できない時間帯である事を知らせるメッセージを表示されます。

コンピュータ利用時間の監視

選択したユーザーがインターネットにアクセスできる時間を指定します。

まず、**コンピュータ利用時間の監視**にチェックを入れます。次に、ユーザーにコンピュータ使用を許可する時間数を、週と月ベースで設定し、さらに特定の曜日に許可する時間数も設定します。

例えば、週末と平日で異なった利用時間を許可したりするように設定できます。 許可する **時間** を **日 / 時 : 分** の欄に入力します。例えば**「04 / 20 : 05」** と入力すると、コンピュータの使用時間は「4 日間、20 時間と 5 分」となります。

時間切れの前に警告を表示にチェックをいれると、コンピュータが自動的にシャットダウンされる前に、ユーザーにその旨を知らせることができます。コンピュータが事前の警告なしにシャットダウンされると、データの消失の原因になります。

コンピュータ利用時間の監視では複数の矛盾する数値が入力された場合、常に最小値が適用されます。1 か月の時間制限を 4 日間に設定したのに 1 週間の時間制限を 5 日間と設定した場合、ユーザーのコンピュータ利用時間は4 日間に制限されます。

パーソナルフィルタ

自分で作成した**ホワイトリスト**（許可するコンテンツ）と**ブラックリスト**（禁止するコンテンツ）の新規作成や変更ができます。

- **ホワイトリスト**: 選択したユーザーに対してホワイトリストを選択すると、このユーザーはそのホワイトリストに登録されているウェブページにしかアクセスできません。**マスタデータ**領域では、管理者はホワイトリストをそれぞれのユーザーにカスタマイズしたり、既存のホワイトリストからそれぞれのユーザーに合ったリストを選択できます。ホワイトリストは、特に、幼少の子供がアクセスできるサイトを絞り込み、教育上有益なコンテンツを掲載するウェブページを利用させるために役立ちます。
- **ブラックリスト**: ブラックリストはユーザーに特定サイトへのアクセスを禁止します。ブラックリストで指定した以外のコンテンツには、自由にアクセスできます。例えば、ブラックリストで指定したサイトと類似したコンテンツを含むサイトにはアクセスできます。

ホワイトリストとブラックリストの編集には以下のボタンを使用します。

- **削除**: マウスで選択したリストを削除します。
- **新規作成**: ブラックリストまたはホワイトリストを新規作成します。作成方法は、禁止するコンテンツ および 許可するコンテンツ の項を参照してください。操作方法については、禁止するコンテンツおよび許可するコンテンツの説明を参照してください。
- **編集**: 既存リストの内容を変更します。

ログ

ログ領域では、管理者は各ユーザーの接続履歴、拒否されたコンテンツの内容やブロックした理由などの情報を確認できます。

「ログを削除」をクリックすると、ログは消去されます。

設定: このアイコンをクリックすると、ログに関する設定が表示されます。ログが記録される対象ユーザーは、フィルタリングが有効かつコンピュータ上に作成されたユーザーとなります。

使用環境によっては、ログファイルの容量が非常に大きくなります。ログファイルがディスク容量を圧迫するようであれば、**ファイルが__KBに達したときにメッセージを表示**にチェックを入れて、適当な数値を入力してください。ファイルのサイズが、設定された数値に到達すると、ユーザーに通知します。ログを削除する場合は、ログ領域の**「ログを削除」**から削除できます。

ヒント集

本製品を利用する上での重要なヒントをまとめました。

ブートスキャンの流れ

ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。本製品には、Windows 起動前にスキャンを実行できるブートスキャン機能が搭載されています。

ブートとは
コンピュータの電源を入れると、通常は自動的に Windows OS が起動します。このプロセスを「ブート」と呼びます。しかし、Windows OS の代わりに別のプログラムを自動的に起動させることができます。コンピュータで Windows が起動する前にウイルススキャンできるように、本製品では Windows バージョン以外に、ブート可能なバージョンが用意されています。

ブートスキャンを中断するには
再起動後に通常の Windows 起動画面が表示されない場合は、矢印キーを使って、**Microsoft Windows** を選択し、**Enterキー**を押します。そうすると、Windows が通常とおり起動します。

ブートスキャンを実行するには、以下の手順に沿って行ってください。

1a CD版 でのブートスキャン： **製品CD** を使用してコンピュータをブートします。**製品CD** をCDトレイに挿入します。表示された起動ウインドウで、**「キャンセル」** をクリックし、コンピュータをシャットダウンします。

1b ダウンロード版製品でのブートスキャン： **本製品のプログラムグループ（スタート > プログラム > G Data）からG Data ブートCD を作成**を選択して、新しいブートCD を作成します。

作成が完了したら、作成したブートCD をCDトレイに挿入して、コンピュータをシャットダウンします。

※ブートCDの挿入後に起動画面が表示された場合は、**「キャンセル」**をクリックしてコンピュータをシャットダウンします。

※Windows XP 上では、ブートCDの作成時に**「IMAPI 2.x がインストールされていません」**というメッセージが表示されることがあります。これは、データをメディアにコピーするために必要な Microsoft の更新です。Microsoftのサイトからダウンロードしてインストールしてください。

1c **USB版でのブートスキャン:** USBメモリから直接ブートスキャンできます。ただしこのブートスキャンを実行するには、コンピュータがUSBメモリからブートできる状態でなければなりません。**製品USBメモリ** をコンピュータのUSBポートに差し込みます。表示された起動ウインドウで **「キャンセル」**をクリックし、コンピュータをシャットダウンします。

手順 1 （a, b, c）の後は、ブートスキャンの手順は各パターン共通で次のとおりです。

2 コンピュータを再起動します。**G Data ブートスキャン**のスタートメニューが表示されます。

3 矢印キーで **G Data ブートCD** を選択し、**Enter** キーで確定します。そうすると、自動的に Linux OS が起動し、ブートスキャン用画面が表示されます。

プログラム画面が正常に表示されない場合には、コンピュータを再起動して **G Data BootCD - Alternative** を選択してください。

4 **ワクチン**を更新するよう促されます。

バックアップが利用できる製品では、ここからバックアップの復元を開始することができます。

5 **「はい」**をクリックして更新を実行してください。インターネットを介してデータが更新されると、**「更新できました」**というメッセージが表示されます。**「閉じる」**をクリックして更新画面を閉じます。

自動インターネット更新機能は、IP アドレスを自動割当機能（DHCP）を持つルータを使用している場合にのみ、利用できます。インターネット更新が利用できなくても、古いワクチンを利用して、ブートスキャンを実行できます。ただし、この場合には、本製品のインストール後できるだけ早いうちに、更新したワクチンを使って、ブートスキャンを実行してください。

6 プログラムの画面が表示されます。**「コンピュータをスキャン」**をクリックすると、スキャンが開始されます。

7 **ウイルスが検出されたら**、本製品が提案する処理方法から適当なものを選択して、ウイルス駆除を行ってください。ウイルスを駆除できたら、オリジナルファイルが再び使用可能な状態になります。

なお、ファイルがシステムファイルや重要なファイルと思われる場合は、削除しないことをお勧めします。※削除を選択する場合は、対象のファイルが削除されてもシステムに問題を引起さないことを確かめてから、操作を実行してください。

8 ウイルススキャンが完了すると、画面右上の X マークをクリックして、終了してください。

9 CD ドライブのトレイが開いたら、**製品CD** を取り出します。（**USB メモリ** を使用してブートスキャンしている場合は、コンピュータのUSBスロットに差し込まれているUSBメモリを抜きます。）

10 コンピュータを再起動し、通常通り Windows OS を起動します。

コンピュータを CD-ROM からブートできない場合

コンピュータを CD/DVD-ROM からブートできない場合、まずこのオプションを設定する必要があります。この設定は、BIOS と呼ばれる Windows OS の前に自動的に起動するシステム内で行います。BIOS に変更を加える手順は次のとおりです。

1. コンピュータをシャットダウンします。
2. コンピュータを起動します。通常 BIOS 設定を行うには、コンピュータが立ち上がる（= ブート）時に **Delete** キー（F2 キーまたは F10 キーの場合もあります）を押します。

3. BIOS の各設定項目をどのように変更するかはコンピュータによってさまざまですので、コンピュータの取扱説明書をお読みください。変更後のブート順を CD/DVD-ROM: C: にします。したがって、CD/DVD-ROM ドライブが [1st Boot Device] （第 1 ブートデバイス）となり、Windows OS がインストールされているハードディスクパーティションは 2nd Boot Device （第 2 ブートデバイス）になります。
4. 変更を保存して、コンピュータを再起動します。これでブートスキャンできる状態になりました。

コンピュータを USBメモリ からブートできない場合

コンピュータを自動的に USB メモリからブートできない場合には、以下のどちらかの手順に従ってください。

手順 1 （推奨）

1. コンピュータをシャットダウンします。
2. 製品USBメモリ をコンピュータの空いている**USBポート**に差し込みます。
3. コンピュータを起動します。
4. ブート時に、**ブートメニュー表示用のキー**（機種によって異なるので、コンピュータの説明書を確認ください）を押して、ブートメニューを開きます。
5. ここで、挿入したUSBメモリを選択し、**Enter** キーを押します。
6. これでUSBメモリから起動します。

手順 2

1. コンピュータをシャットダウンします。
2. 製品USBメモリ をコンピュータの空いている**USBポート**に差し込みます。
3. コンピュータを起動します。
4. ブート時に **F2** キーを押して、BIOS セットアップ画面を開きます。
5. BIOS 画面のメニューバーで **Boot** を選択します。メニュー項目を選択するには、左右矢印キーでカーソルを移動します。選択項目にカーソルを合わせ、**Enter** キーを押します。

6. ここで、上下矢印キーで **Hard disc drives** を選択します。選択項目にカーソルを合わせ、Enter キーを押します。
7. そして **USB** を選択すると、**1st Drive = USB** が一番上にきます（矢印キーでカーソル移動、Enter キーで選択）。
8. **F10** キーを押して変更を保存し、BIOS セットアップ画面を閉じます。これでネットブックが USB メモリからブートできる状態になりました。
9. コンピュータを**再起動**します。これでコンピュータのブートスキャンを実行できます。

G Data アイコン

本製品の保護機能が有効に設定されているかどうかは、タスクバー上の G Data アイコンで確認できます。

このアイコンが表示されている時は、G Data によるセキュリティ保護が有効で、コンピュータが適切に保護されていることを意味しています。

警告マーク付きのアイコンが表示される時には、セキュリティ保護が有効になっていないことを意味しています。このアイコンは、ウイルスガードを無効にしたり、セキュリティ保護に問題がある場合に表示されます。

このアイコンが表示されている時は、本製品がインターネットから更新ファイルをダウンロードしています。

G Data アイコン上で右クリックをすると、右クリックメニューが表示されます。右クリックメニューからは、ユーザーがよく使用する操作が選択できます。

次のような操作が選択できます。

- **G Data （製品名） を起動**: 本製品プログラムのセキュリティセンターを呼び出します。セキュリティセンターに関する詳細は、セキュリティセンターを参照してください。

- **ウイルスガードを無効にする**: ウイルスガードの有効／無効を切り替えます。大容量のファイルをコピーしたりする際にウイルスガードを無効にすると処理がより高速に行われますが、ウイルスガードを無効にする期間は最小限に抑えてください。またウイルスガードが無効な間は、インターネットやスキャン未実行のメディアと接続しないようにしてください。

- **ファイアウォールを無効にする**: ファイアウォールが搭載されている製品では、右クリックメニューからファイアウォールの有効／無効を切り替えることができます。インターネット接続環境では、ファイアウォールを無効にした後も、コンピュータは引き続きインターネットに接続され、外部からの攻撃から保護されません。ファイアウォールを無効にする際は注意してください。

- **オートパイロットを有効にする**: ファイアウォールのオートパイロット機能の有効／無効を切り替えます。オートパイロットを無効にすると、ネットワーク接続についてユーザーへ確認が行われるようになります。通常はオートパイロットは有効にした状態で利用することをお勧めします。

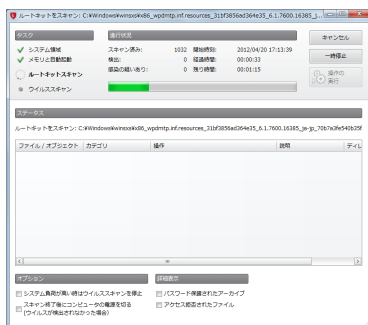
- **ワクチンを更新**: 今すぐにワクチン更新を手動実行します。コンピュータの適切な保護には、ワクチン更新は非常に重要です。ワクチン更新は、通常は自動更新に設定しておいてください。インターネット更新に関する詳細は、更新の項を参照してください。

- **統計情報**: メール、ウェブ、ウイルスガードなどのスキャン統計を確認できます。

ウイルススキャンの流れ

ウイルススキャンは、コンピュータ上のマルウェアをスキャンする機能です。ウイルススキャン中にウイルスが検出されると、検出されたウイルスへの対処方法を選択できます。

1. ウイルススキャンを開始します。ウイルススキャンの開始方法は、ウイルススキャンの項を参照してください。

2. コンピュータ上でスキャンが始まると、スキャンのステータス情報を表示する画面が開きます。

画面上部のステータス表示バーには、スキャンの進捗状況が表示されます。ウイルススキャンのプロセスに関する設定は、スキャン中に行うことができます。設定できる項目は次のとおりです。

- **システム負荷が高い時はウイルススキャンを停止**: ユーザーがコンピュータで作業を行っている間は、ウイルススキャンを自動的に停止します。
- **スキャン終了後にコンピュータの電源を切る**: ウイルススキャン終了後に、コンピュータが自動的にシャットダウンします。

- **パスワード保護されたアーカイブ**: アーカイブがパスワードで保護されている場合、このアーカイブはスキャンされません。ここにチェックを入れると、スキャンできなかったパスワード保護されたアーカイブを表示します。これらのアーカイブにウイルスが潜んでいたとしていても、解凍しない限り、ウイルスがシステムに感染する可能性はありません。

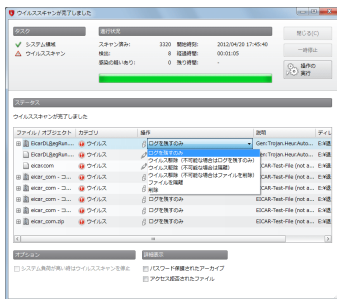
- **アクセス拒否されたファイル**: アプリケーション自身の動作のために使用する Windows ファイルは、そのアプリケーションの実行中はスキャンできません。スキャン実行中は、可能な限り、他のプログラムを実行しないようにしてください。ここにチェックを入れると、スキャンできなかったデータが表示されます。

3a ウイルススキャン結果が画面に表示されます。ウイルスが検出されなければ、**「閉じる」**をクリックして画面を閉じます。

3b **ウイルスが検出された場合**は、**「操作の実行」**をクリックして感染ファイルの処理を行います。

デフォルト設定では、感染ファイルからウイルスを駆除します。ウイルスを駆除したファイルは再び普通に使用してもコンピュータに支障をきたしません。

駆除できない場合には、ファイルは隔離領域に移動されます。隔離されたファイルは、暗号化して保存されるので、コンピュータに問題を引起すことはありません。この感染ファイルが必要にな場合は、隔離領域から元の場所に戻して使用できます。

3c 感染ファイルやオブジェクトが、必要か不要がを判別できる場合には、スキャン結果 1 件ごとに操作を実行することもできます。

スキャン結果一覧の**「操作」**で、感染ファイル 1 件ごとに処理方法を決めます。

- **ログを残すのみ**: 感染したファイルを**ログ**として記録します。感染ファイルのウイルス駆除やファイル削除はされません。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合はログを残すのみ）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、このログを基に後で処理方法を決めることができます。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合は隔離）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、**隔離**します（推奨設定）。隔離に関する詳細は、**隔離でできること**を参照してください。
- **ウイルス駆除（不可能な場合はファイルを削除）**: 感染ファイルからウイルスを駆除できなかった場合は、ファイルを削除します。この処理方法は、コンピュータ上に重要なデータが無い場合にのみ選択してください。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。
- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離**領域に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、**隔離でできること**を参照してください。
- **削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

「操作を実行」をクリックすると、ウイルス検出のたびに、ユーザーが設定した処理が行われます。

4 スキャン終了後は、感染ファイルのコピーを G Data に送信できます。コピーを送信すると、ご利用の製品の更なる品質向上に役立つので、できるだけ送信するようにしてください。

感染ファイルの送信は、飛ばすことも可能です。今後感染が見つかった場合で、この画面が今後表示されないように設定することもできます。

ウイルスが検出された時の対応

ウイルスまたは他の不正プログラムが発見された場合、感染ファイルを以下の方法で処理します。

- **ログを残すのみ**: 感染したファイルを**ログ**として記録します。感染ファイルのウイルス駆除やファイル削除はされません。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合はログを残すのみ）**：感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、このログを基に後で処理方法を決めることができます。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合は隔離）**：感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、**隔離**します（推奨設定）。隔離に関する詳細は、**隔離でできること**を参照してください。
- **ウイルス駆除（不可能な場合はファイルを削除）**：感染ファイルからウイルスを駆除できなかった場合は、ファイルを削除します。この処理方法は、コンピュータ上に重要なデータが無い場合にのみ選択してください。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。
- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離**領域に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、**隔離でできること**を参照してください。
- **削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

  ※メールの受信トレイ用のアーカイブは隔離しないでください。受信トレイのアーカイブが隔離されると、メールプログラムはメールデータにアクセスできなくなり、メールプログラムは適切に機能しなくなります。

ウイルススキャンで「not-a-virus」が表示される

「not-a-virus」 と表示されるファイルは、ファイル自身は不正機能を持っていませんが、ある状況においては攻撃者によって不正利用され、コンピュータに危害を加えられる可能性があるアプリケーションです。

not-a-virus カテゴリには、キー配列自動変更ツール、IRCクライアント、FTPサーバー、プロセス作成（または隠す）ツールなどあります。

隔離でできること

ウイルス検出時の処理方法の１つに**隔離**という処理方法があります。この操作を行うと、検出されたファイルが他のファイルに危害を及ぼさないように、コンピュータ上に作成された暗号化領域に保存されます。

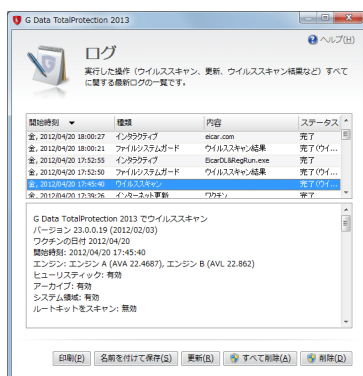
隔離領域に移動したファイルは、検出された時の状態で保存され、隔離ファイルには次の操作が可能です。

- **更新**: 隔離情報を更新します。隔離画面を開いてからかなり時間が経過して、他にもウイルスが検出された場合、それらを表示します。
- **送信**: 感染ファイルを G Data に送信します。感染ファイルが新種の不正ファイルである場合は、その後のワクチン開発に活用されます。ユーザーが送信した情報は匿名情報として処理されます。詳細は、マルウェアフィードバック を参照してください。
- **ウイルス駆除**: 感染ファイルから感染部分のみを駆除し、ファイルを元の場所に戻します。場合によっては、駆除はできない場合もあります。

- **元に戻す**: 隔離ファイルを元に戻します。この処理は例外ケースを除き利用しないでください。利用する場合は、コンピュータのネットワーク／インターネット接続を切断し、未感染データをバックアップするなどした上で、実行してください。
- **削除**: 感染ファイルが不要な場合は、隔離領域から削除できます。

ログ

ログ領域では本製品が作成したログが表示されます。

列見出しの **開始時刻**、**種類**、**内容** もしくは**ステータス**をクリックすると、ログを並び替えることができます。**「名前を付けて保存」**では、ログをテキストファイルに保存し、 **「印刷」**ではログを印刷できます。ログを削除するには、対象をマウスで選択してから、 **「削除」**ボタン（もしくはキーボードの**削除キー**）を押してください。

複数台用ライセンスを所有している場合

複数台用ライセンスをご購入いただくと、取得したライセンスと同数のコンピュータに 本製品をインストールして使用できます。1 台目のコンピュータへのインストールとインターネット更新が終了すると、メールでアクセスデータが送信されます。そして 2 台目のコンピュータにもソフトウェアをインストールする時には、G Data 更新サーバー に登録した時に発行されたユーザー名とパスワードを入力します。3 台目以降のコンピュータにもこの作業を繰り返します。

製品の初回登録時に発行されたインターネット更新用の**アクセスデータ**（ユーザー名とパスワード）を、すべての PC で使用してください。手順は以下のとおりです。

1 本製品を起動します。

2 セキュリティセンターで**更新**をクリックし、プルダウンメニューから **ワクチンの更新**をクリックします。

3 表示されるウィンドウに、G Data から送られてきたメールで送信されたアクセスデータを入力します。「OK」をクリックすると、更新ができるようになります。

ライセンスの期限が切れた場合

ライセンスの期限切れが近づくとポップアップのメッセージでお知らせします。このポップアップメッセージをクリックすると、ダイアログが開き、ここから更新の手続きを行うことができます。

更新手続きは、G Data ウェブサイトからも可能です。

コンピュータを買い替えたり、クリーンインストールした場合

コンピュータを買い換えたり、クリーンインストールした場合は、本製品をコンピュータにインストールし、初回登録時に G Data から送付されたアクセスデータを入力します。アクセスデータの入力は、インストールもしくは更新を参照してください。

ライセンスの移行には回数制限が設定されています。この回数を超えた場合は、更新期限が有効でも更新がロードできなくなりますので、ユーザーサポートに問い合わせください。

アンインストールの方法

本製品をアンインストールする場合は、Windows タスクバーの [スタート] > [プログラム] > [G Data] から [アンインストール] をクリックすると、ダイアログ形式で簡単にアンインストールを実行できるようになっています。なお、以下の手順で、Windows のコントロールパネルからもアンインストールは可能です。

- Windows 8: スタート画面（Modern UI）から、本製品のアイコンを右クリックし、画面下の［**アンインストール**］を選択します。表示された［**プログラムと機能**］ウインドウから、本製品を選択し、［**アンインストール**］をクリックしてアンインストールを実行します。

- Windows Vista, Windows 7: Windows タスクバーで **[スタート]**（通常はディスプレイの左下に配置）をクリックし、**[コントロールパネル]** を選択します。 そこで [プログラム] > [プログラムのアンインストール] を選択します。表示されたリストから 本製品を選択し、**[アンインストール]** をクリックしてアンインストールを実行します。

- Windows XP: Windows タスクバーの **[スタート]** をクリックして [設定] > [コントロールパネル] > [プログラムの追加と削除] を選択します。表示された **[プログラムの追加と削除]** ウインドウから、本製品をマウスで選択します。そして **[変更と削除]** をクリックしてアンインストールを実行します。

隔離済みファイルが隔離領域に残っていると、アンインストール中に、これらファイルを削除するかどうかを確認されます。隔離ファイルを削除しない場合は、当該ファイルは暗号化されて**G Data フォルダ**に保存され、アンインストール後もコンピュータ内に残ります（これらのファイルは本製品を再インストールしないと使用できません）。また、アンインストール中に、**設定とログ**を削除するかどうかについても確認されます。これらのファイルを削除せずにコンピュータに残しておくと、ソフトウェアを再インストールした場合、保存されたログと設定が再び使用できるようになります。

「終了」をクリックすると、アンインストールを終了します。これでソフトウェアがシステムから完全にアンインストールされます。

ウイルス被害に遭わないために

本製品には、業界最高水準の技術が搭載されており、既知ウイルスだけでなく、未知ウイルスに対して高い検出率を誇っています。最善の保護を実現するには、ウイルス対策ソフトのインストールの他に、コンピュータを使用するにあたって、日ごろからのユーザーの心がけも重要です。

ここでは、システムやデータの安全性を更に向上させる対策方法を紹介します。

- **複数のユーザーアカウントを使用する**: コンピュータにユーザーアカウントを 2 つ作ります。ひとつは**管理者アカウント**で、ソフトウェアをインストールしたりコンピュータの基幹的な設定を行う時にはこのアカウントを使用します。もうひとつは権限に制約のある**ユーザーアカウント**です。このユーザーアカウントでは、プログラムのインストールや Windows OS の変更をできないように権限を制限しておきます。このアカウントでログインすれば、比較的安全にインターネットや別のコンピュータからのデータ取得などを行うことができます。複数種類のユーザーアカウントを作成する方法は、Windows OS のヘルプを参照してください。

- **スパムメールを無視する**: チェーンメールやスパムメールに含まれているリンクや添付ファイルは、絶対開かないでください。また、これらのメールへの転送や返信もしないでください。

- **ウイルス感染の可能性がある場合は、すぐにスキャンする**: 新しくインストールしたソフトウェアが動作しない、またはエラーメッセージが表示されるなど、ウイルス感染が懸念される場合には、再起動する前に、問題のプログラムをスキャンしてください。再起動の前にスキャンする理由は、トロイの木馬は通常コンピュータの再起動時に削除コマンドを実行するので、再起動前にスキャンを実行する方がウイルスを検出、駆除できやすいためです。

- **定期的に Windows やソフトウェアを更新する**: 新種ウイルスは、古くなったソフトウェアの脆弱性をついて攻撃を仕掛けてきます。それを防ぐために、Microsoft や各種ソフトウェア開発元から新たなパッチが提供されたら、速やかにダウンロードしてコンピュータにパッチをあてましょう。パッチを適用することで、Windows や各種ソフトウェアの脆弱性は修正され、攻撃者が脆弱性を利用した攻撃から防御できます。なお、Windows の更新は自動的に実行されるように設定しておき、その他のソフトウェアに関しても自動更新を利用する事をお勧めします。

- **オリジナルのソフトウェアを使用する**: ファイル共有サイトなどで出回って

いるソフトウェアは、ウイルス感染している可能性が非常に高いことが各種の分析や調査で実証されています。プログラムは必ずオリジナルのものを使用してください。出所の怪しいプログラムのダウンロードや利用は避けてください。

- インターネットからダウンロードしたソフトウェアの取り扱いに注意する
: ソフトウェアをインターネットからダウンロードする際には、ダウンロード先のサイトの信頼性に十分に注意を払い、信頼できる供給元のソフトウェアだけを使用してください。また、心あたりのない送信者や、友人や同僚から予期せず届いたメールに含まれる添付ファイルは、決して開かないようにしましょう。ファイルを開く場合は、事前に送信者に確認をして、その安全性を確保してください。

データ保護に関する声明

G Data アンチウイルス 2013、G Data インターネットセキュリティ 2013、および G Data トータルプロテクション 2013 のデータ保護に関する声明

G Data製品には、特定条件件下においてデータをG Dataのクラウドサーバーへ送信する保護コンポーネントが含まれています。保護コンポーネントのコア機能を正常に機能させるために必要な特定データは、常に同サーバーへ送信されます。保護コンポーネントの１つ、ウェブ保護には、ウェブサイトのアドレス送信が必須となります。また、別の保護コンポーネント、バンクガードでは、新種のバンキング系トロイの木馬の特定・削除のために、チェックサムの送信が必要となります。更に、ふるまい検知（ビヘイビアブロッカー）の機能は、クラウドからの情報を取得することにより、コンピュータをより効果的に保護できますが、これには、不審なファイルに関する特定の情報をクラウドサーバーへ送信する必要があります。

また、送信されるデータは、他のコンポーネントにおいても重要な意味を持っています。ユーザー様から送信されたデータは、G Dataのセキュリティラボで有害なファイルを検証や挙動の分析に使用されます。検証結果は、G Dataの保護コンポーネントの改善やG Data製品のユーザーへの有害プログラムに関する情報やその影響を提供します。詳細は、マルウェア情報イニシアチブ（MII）のデータ保護に関する声明をご覧ください。なお、MIIへの参加は任意です。MIIへの参加を無効化しても、G Dataによる保護メカニズムは、その効果を制限されません。

重要：　これらの機能で収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

・ウェブ保護によるデータ収集

G Data ウェブ保護とは?

インターネットには、数多くの有害サイトや詐欺サイトが存在しています。これらのサイトは、マルウェア配布や適切な保護が施されていないコンピュータを感染させるための感染経路（Drive-By-Infection）として使われており、個人情報を盗み出したり（例： Paypalや Facebookのサイトフィッシング）、スキャムなどの詐欺として使用されている可能性があります。G Dataは、有害サイトへのアクセスを遮断するブラックリストを独自に管理・保守しています。G Dataウェブ保護は、次の2種類のテクノロジーがベースとなっています。

1. HTTPスキャン。この機能は、既知の有害コードがないか、ウイルススキャナでスキャンしてHTTPトラフィックをチェックする機能です。有害コードが見つかった場合、G Dataが警告を発します。なお、警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

2.フィッシング保護。この機能は、リクエストされたアドレスがフィッシングサイトではないか、G Data が管理・保守するブラックリストと照合し、フィッシングサイトであった場合は警告を発する機能です。このURLブラックリストには、無数の有害サイトや詐欺サイトの情報が保存されています。なお、フィッシング警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

収集される情報の種類は?

リクエスト先のウェブサイトがG DataのURLブラックリストに存在するかチェックするため、ウェブサイトのアドレスをクラウドサーバーに送信します。

収集された情報の使用方法は?

リクエスト先のアドレスは、G Dataのデータベースに保存されますが、リクエスト送信元のユーザーもしくはPC情報は保存されません。ウェブサイトのアドレスは、まずG Dataの分析システムに転送され、次のステップで、有害もしくは不審な構成部分をチェックします。不審なウェブサイトのアドレスは、G Dataセキュリティラボの分析システムに転送されます。分析によって不審サイトと確認された場合は、このサイトはブラックリストに追加されます。

G Dataのクラウドサーバーとリクエスト送信元コンピュータの間の接続中は、送信元コンピュータのIPアドレスが送信されますが、通常、このIPアドレス情報はG Data側では保存されません。ウェブサイトがブロックされた場合は、IPアドレスをもとに国情報を識別しますが、IPアドレスは識別後に破棄します。そのため、G Data側でリクエスト送信元の個人を特定することはできません。

・G Data バンクガードによるデータ収集

G Data バンクガードとは?

G Data バンクガードは、ブラウザのメモリ領域が破損状況やマルウェアによる改竄など、ブラウザが暗号化された情報の送信に使用するシステムライブラリを監視する機能です。G Data バンクガードがこの領域への攻撃を検出すると、保護メカニズムが作動し、攻撃されたブラウザを通常ステータスに戻します。その後、攻撃を引き起こした有害ファイルをシステムから見つけ出し、除去します。

収集するデータの種類は?

ブラウザのメモリが攻撃された場合、次の情報が送信されます 。

バージョン番号

- G Data 製品および同コンポーネント
- ブラウザおよび同コンポーネント
- OS情報

チェックサム

- 攻撃元および攻撃に関わったファイル
- 削除されたファイル

匿名 GUID

- 発生した事象を特定のコンピュータを関連付けるため、コンピュータのGUID情報を取得します。なお、GUIDは同一の情報が存在する可能性は非常に低く、GUIDからコンピュータの場所や個人の特定はできません。

攻撃時のアクティビティ情報

- 攻撃を特定マルウェアに関連付けるため、攻撃種類をもとにマルウェアを特定するフィンガープリントを取得します。フィンガープリントはシステムライブラリの呼び出しに基づくもので、これには個人情報は含まれません。
- 各システムライブラリで危険にさられている機能の名称

マルウェア除去時のアクティビティ情報

- 削除されたレジストリエントリ
- 削除時: ルートキットの種類（例： Watchdog/Versteck via Hook)

収集された情報の使用方法は?

バージョン番号は、発生した事象とプログラムバージョンを関連付けるために使用します。これは、エラー発生数の減少と脆弱なシステムの特定に役立ちます。

関連付けられたファイルのチェックサムは、G Dataのデータベース内の有害ファイルとの照合やさらに詳しい分析を行う上で、役立ちます。G Dataが保しない新たな脅威が発生した場合、この脅威は、リクエストリストへと入れられます。そして、次にこの脅威へのリクエストが確認された場合、実際にファイルが転送されます。このリクエストは、同じコンピュータから複数回送信されることはほぼありません。このリクエストは、実行可能なファイルの場合にのみ、送信されます。ドキュメント、画像、またはその他の個人情報を含むファイルなどは、送信されません。

フィンガープリントで、マルウェアを特定の系種に識別できます。同じ系種に属するマルウェアは同様の手法を用いて駆除できます。

クラウドサーバーとリクエストされたコンピュータ間の接続中は、リクエストされたコンピュータのIPアドレス情報が取得されますが、これは保存されません。ウェブサイトが有害と判定された場合、このIPアドレスを用いて、リクエスト元の国情報を取得します。このプロセスの後、IPアドレスは破棄されるため、G Data でユーザー情報の詳細を特定することはできません。

攻撃時のアクティビティ、更に攻撃に関わったり、削除されたファイルおよびレジストリエントリの情報は、削除ルーチンの分析・開発に役立ちます。これらのデータを使うと、新たな脅威や攻撃に迅速に対応できるようになります。

特定のデータは統計に使用されます。系種別の出現頻度などはG Dataのホワイトペーパーやマルウェアレポートで使用されます。また、これらの情報は、作業プロセスの優先度の決定や自動化にも使われています。

・ふるまい検知およびファイルクラウドセキュリティによるデータ収集

ふるまい検知とは?

ふるまい検知は、コンピュータ上のすべてのアクティブなプログラムによる不審な動きを監視する機能です。ふるまい検知では、プログラムによる挙動がすべてポイントで計算され、特定の値を超えると、当該プログラムを終了に導きます。特定の条件下においては、ふるまい検知は不審なファイルのチェックサムをG Dataのサーバーへと送信し、既知のマルウェアファイルと照合します。チェックサム送信の条件は、プログラムのダウンロード時、プログラムの初回起動時、プログラムによるある程度の不審な動きが実行された場合などがあります。ファイルが有害であると判断された場合は、プログラムの実行を中止するかどうか、ユーザーに確認します。

収集するデータの種類は?

ファイルをチェックする場合、チェックサム情報を取得し、サーバーに送信します。更に、ふるまい検知が有害度評価のために取得されたパラメーター（例: 有害度（0-1）、評価したルールのID番号）が送信されます。ファイルが有害と判定された場合、プログラムの呼び出しパラメーターが取得されます。警告メッセージに対するユーザーの操作情報も送信されます。また、ログ、ルールセット、G Data製品のバージョン番号も送信されます。

収集された情報の使用方法は?

有害度の数値（チェックサムによって識別）は、有害なファイルをG Dataが保するマルウェアデータベースでの照合に使用します。このファイルは、ピンポイントで分析され、場合によっては、ブラックリストでブロックされます。ユーザーの操作情報は、誤検出の発見や修正に役立ちます。

・G Data マルウェア情報イニシアチブの収集データのデータ保護に関する声明

上で述べた保護コンポーネントで必要なデータを除き、マルウェアイニシアチブでは、参加に協力頂いたユーザー様から、以下の情報を収集しています。これらの情報は、保護メカニズムの分析・開発の迅速化に役立つので、ぜひ参加にご協力ください。

G Data マルウェア情報イニシアチブとは?

G Data セキュリティラボでは、G Data 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG Data の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G Dataマルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG Dataセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG Data製品をご利用の方々もインターネットをより安全に利用できるようになります。

収集される情報の種類は?

原則として、次の３種類のデータ収集方法があります。

1. G Dataの保護メカニズム（ウイルススキャナ、ふるまい検知、バンクガードなど）が、ユーザー様のコンピュータ上で有害ファイルが検出された場合（送信する情報は保護メカニズムによって異なります）
2. ウェブサイト上で有害なコンテンツが発見された場合
3. ユーザー様自身が任意でG Data セキュリティラボにデータを送信した場合

ユーザー様がマルウェアファイルをG Data セキュリティラボへ送信すると、システムは送信されるファイルのほかに、ワクチン情報、スキャンエンジンのバージョン番号、発見場所、オリジナルのファイル名、作成日という情報が一緒に送信されます。

有害なインターネットコンテンツを検出した場合は、次のデータが送信されます。

- マルウェア情報のバージョン
- G Data 製品および使用スキャンエンジンのバージョン番号
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- ブラウザのユーザーエージェント
- アクセスを遮断したURLと遮断した理由（マルウェアサイト、フィッシングサイトなど）
- マルウェア名

不審な実行可能ファイルが検出された際は、次の情報を取得します。また、検出したファイルは、送信することもできます。

- 有害または不審なファイルのチェックサム
- ファイルサイズ
- ファイルに署名されている場合は、証明書の情報

- 攻撃に関わった有害または不審なファイルの検出場所
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- 攻撃後に削除されたファイルの匿名パス
- 特定の条件下（G Dataが未所の新たな脅威が発生した場合）では、攻撃に関わったファイルのダウンロードをG Dataが要求することができます。送信されるファイルは、攻撃に関わっている実行可能なファイルのみです。

重要：　収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

収集したデータの利用方法は?

データの処理および保存にあたっては、各国で適用されるデータ保護ならびに開示に関する法規が適用されます。 G Dataは、すべてのデータを不正アクセスから保護するため、厳重にデータを管理します。

ウェブサイトのアドレス情報は、まず選定が行われますが、有害または詐欺サイトの共通点を突き止める用途に使用されます。分析結果はURLブラックリストやG Data の他の保護メカニズムにも反映されます。特定のデータは、統計分析や開発などに使用されます。

不審なファイルに関する情報は、G Data で関連ファイルとの照合や有害プログラムの挙動を分析に使用します。取得した情報は、詳しい分析を行うためのベースとなる重要な要素です。目的は、保護メカニズムによる保護や駆除機能の改善となります。

有害プログラムの挙動を検証するには、有害ファイルが必要です。このため、ファイルをG Dataに送付することができます。送信するファイルは、実行可能なファイルのみです。文書やデータベースなど個人情報を含むファイルは送信されません。更に、ファイルは２つのステップを踏んで送信されます。まず、最初のステップでは、チェックサムもしくは他の共通プロパティを用い、ファイルをリクエストリストに入れられます。ファイルが再びリクエストされると、アップロードが開始されます。これが第２のステップです。このリクエストが同じコンピュータから発生するケースはほぼありません。ファイルは、その後G Data セキュリティラボで詳しく検証されます。統計データは、優先度の決定（例：頻度が高いほど、優先的に処理）、またはG Dataが作成するレポートに活用されます。マルウェアを削除するツールも、同様となります。

データの評価はG Dataセキュリティラボ内で行われ、評価結果はITセキュリティ分野の研究事案の解明にのみ利用されます。 収集データ利用における最大目標は、安全上のリスクの研究と保護メカニズムの開発です。 収集したデータの評価結果は例えば、ブラックリストの作成、専門記事発表のための統計、セキュリティ技術用ルールの開発などに利用されます。 このイニシアチブへの参加は任意であり、参加されなくてもご利用頂く製品の機能に影響がでることはありません。 G Dataマルウェア情報イニシアチブにご参加頂くことにより、今後すべてのG Dataユーザーがコンピューターへの脅威について、より詳細な情報を得ることができるようになるとともに、ご利用のコンピュータの保護精度が向上します。

G Data製品によるデータ収集へのご理解とマルウェア情報イニシアチブ参加へのご協力頂きますよう、何卒宜しくお願い申し上げます。

使用許諾契約

G Data Software AG （以下、「G Data」）は、本使用許諾契約書のすべての条項に同意することを条件に、本ソフトウェア（以下、「本製品」）の使用許可をユーザー（以下、「ライセンス契約者」）に保証します。本使用許諾契約書に同意することによって、ライセンス契約者とG Dataの間に法的契約が締結されます。契約書の内容をよくお読みになってから、本製品をご利用ください。本契約書の条項に同意しない場合は、インストールを中断し本製品をお使いにならないでください。

1. 定義

「定義ファイル更新」： 製品の認証後にインターネット経由で利用できる機能（例： ウイルス定義ファイル（またはワクチンとも呼ぶ）、アンチスパム用のルール、URLリストなど）

「ドキュメンテーション」： 本製品に付属する関連文書

「ライセンス文書」： ライセンス数やライセンス効期限が記されているG Dataライセンス証明書、G Dataにより発行されたライセンス文書、あるいはライセンス契約者とG Dataとの間の書面による同意書。個人版製品では、ライセンスの適用範囲はパッケージなどに記されています。

「ソフトウェア更新」： インターネット経由で利用できるソフトウェアの新しいバージョンへの更新

「ライセンス」： ソフトウェアを利用できるPC（物理および仮想）の数量。デバイスのRAMにロードもしくはハードディスクなどの記憶領域にインストールされている状態を、ライセンスが「使用されている」とみなします。

「アクセスデータ」： 本製品に含まれているレジストレーション番号、レジストレーション番号の登録後にG Dataから送信されるユーザー名およびパスワード（定義ファイル更新もしくはソフトウェア更新の実行に必要）

2. 使用権

本使用許諾契約書では、G Dataはライセンス契約者に対して、ライセンス文書に記述されているライセンスの数量と効期間で許可される限りにおいて、非独占的、限定的、かつライセンス契約者の所属企業内部での委譲可能な使用権を許諾します。ライセンス契約者は、バックアップ目的での本製品の複製する権利をします。使用権の範囲は、G Dataのライセンス文書で定義された使用期間のすべてのソフトウェア更新および定義ファイル更新に及ぶものとします。

ライセンス契約者は、契約で合意したライセンス数を最大として、本製品をコンピュータにインストールし利用できるものとします。ライセンス文書はライセンス契約者が所持するライセンス数の証明となる文書です。

ライセンス契約者は、本使用許諾契約書の許諾事項を除き、G Dataによる書面の許可なく、（i）本製品の複製、改変、レンタル、リース、サブライセンスの譲渡、または利益の取得や未取得に関わらず、その他の手段を利用して第者に本製品を譲渡、（ii）本製品をベースに派生製品を開発、（iii）リバースエンジニアリング、逆アセンブルまたは逆コンパイル、（iv）第三者へアクセスデータを開示、する権限をさないものとします。

3. 所権

本製品の所権はG Dataもしくはライセンス提供者に帰属し、本製品は著作権法およびその他の知的財産権や国際条約によって保護されています。本製品の複製、修正、拡張および同製品の関連品に関するすべての権利は、G Dataおよびライセンス提供者に帰属し、ライセンス契約者は、これに同意するものとします。上記2の条項における本製品の使用権は、製品の購入によりライセンス契約者に移ります。

4. 保証

G Dataまたは販売代理店は、本製品を記録した記憶媒体もしくはダウンロードによる配布時において、ライセンス契約者に対し、通常の操作および保守条件下においてのみ、媒体もしくはダウンロードした製品がエラーなく動作することを保証します。万一、データ媒体もしくはダウンロードした製品にエラーが存在する場合は、G Dataもしくは販売代理店の定める保証期間内であれば、購入者は代替品の引渡しを要求できるものとします。上記の保証は、事故、不正利用、許可されていない修正、変更、拡張、または不適切な利用方法に起因する損害には適用されません。

上記に明示した保証は、適用される法律の許す限りにおいて唯一かつ排他的な保証であり、特定目的や商品性の保証を含め、その他のあらゆる明示的、黙示的保証に代わるものとします。G Dataは、本製品がライセンス契約者のあらゆる要求を満たす、あるいは如何なる環境においてもエラーが生じることなく動作することを保証しかねます。G DataおよびG Dataのライセンサー、ライセンシー、サプライヤー、または販売業者は、重大過失または明確に法律によって定義された状況を除き、本製品の使用または本ライセンス契約書に直接的または非直接的に関わらず、ライセンス契約者に生じた物質的・非物質的な損害に対し、一切の責任を負いません。なお、補償額は本製品の購入金額を限度とし、人的損害の場合は関連法規に準拠するものとします。

ライセンス契約者は、本製品の利用に関わるあらゆる法規および規定を遵守する責任を負い、本ライセンス契約書の受諾によってこれらを遵守することに同意するものとします。

5. テクニカルサポート

本製品のサポートは、G Dataもしくは販売代理店のサポートもしくはメンテナンスポリシーに準じて提供されるものとします。

6. ライセンス契約の解除

本使用許諾契約は、ライセンス契約者が本契約の条項を遵守しなかった場合、事前の通知なく自動的に失効するものとします。契約者は使用権が失効した時点で、ライセンス契約者は本製品の使用と本製品が記録された媒体を破棄するものとします。

7. 譲渡

事前にG Dataと書面同意し、ユーザーが使用許諾に同意した権利のすべてを譲渡する場合においてのみ、ライセンス契約者は、本契約で保証されている権利とライセンス契約を第者に譲渡できます。

8. ライセンス使用状況の検証

G Dataは、本製品が本使用許諾契約およびライセンス文書に準じた使用を確認するため、通常営業時間に基いた適切な事前通知および最大で1年に1回の履行頻度を条件に、G Dataが任命した守秘義務を課せられた監査人に、ユーザーの本製品に関するインストール状況とその記録の検証を依頼できるものとします。当該検証調査で発生する費用は、ライセンス契約者が使用許可されているライセンス数より5%超過したライセンスを使用している場合を除き、G Dataが負担するものとします。ライセンス契約者が許可されているライセンス数を超過して利用している場合は、ライセンス契約者は当該ライセンスの調査で発生した費用、および超過ライセンス分のライセンス料を負担するものとします。

9. 準拠法

本ライセンス契約書は、ドイツ連邦共和国の法律の解釈に従い、国際物品売買契約に関する国際連合条約の適用は除外されるものとします。本ライセンス契約で定められた一部もしくはすべての規定が無効、またはG Dataにより履行不能である場合でも、本ライセンス契約の残りの規定は引き続き拘束力をするものとします。本契約で定められた権利に対し違反が認められたにも関わらず、G Dataが権利履行を拒絶したとしても、以降の権利放棄を認めるものではありません。

10. サードパーティーのソフトウェア

本製品の一部には、オープンソースおよびフリーライセンスなどのサードパーティーにより開発されたソフトウェアが含まれています。本ライセンス契約は、上述のオープンソースおよびフリーライセンスに適用される権利または義務に対し効力を持ちません。相違する記述または異なる解釈がある場合、本ライセンス契約書の保証制限および保証排除はサードパーティーのソフトウェアに適用されます。

11. 個人情報の取り扱い

a) お客様に関する個人情報は、G Dataが必要な保護措置を講じたうえで、保、利用することにお客様は同意します。

- メールアドレス等、ユーザー登録時に届け出た事項及び、お客様から提出された問い合わせ内容およびアンケートへの回答内容等

b) G Dataが行うサービスにおいて、以下の目的のために個人情報を利用することにお客様は同意します。

- サポートサービスの提供、契約の更新案内、サービスに関する案内（セキュリティ情報等）、G Dataのパートナー他社製品の案内、各種調査、およびキャンペーン、イベントに関する案内、ベータ版テストの依頼等に関する案内

c) G Dataが前項を実施の際、秘密保持契約書を締結したうえで関連会社、販売代理店ならびに代行業者に対し個人情報を開示する場合があることにお客様は同意します。

12. その他の同意事項

本契約および本製品のライセンス文書は、ライセンス契約者とG Dataの間に締結される完全かつ排他的な同意書であり、あらゆる口頭書面による事前同意およびその他の合意における解釈に取って代わるものとします。本契約は、ライセンス契約書もしくは別途作成され、G Dataとライセンス契約者に署名されたライセンス文書もしくはその他の書面による取決めによってのみ、更できるものとします。

索引